AUTHORIZED DOCUMENTATION

Volume I - Guia de Instalação

July, 2008

Novell®
Sentinel®

6.1

www.novell.com

Informações Legais

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentação Online: Para acessar a documentação online mais recente deste e de outros produtos da Novell, consulte a página da Web de Documentação da Novell (http://www.novell.com/documentation).

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Informações Legais de Terceiros

Este produto pode incluir os seguintes programas com código-fonte aberto disponíveis sob a licença LGPL. O texto da licença pode ser encontrado no diretório Licenses.

edtFTPj-1.2.3 foi licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.enterprisedt.com/products/edtftpj/purchase.html (http://www.enterprisedt.com/products/edtftpj/purchase.html).

Enhydra Shark, licenciado sob a Licença Pública GNU Menos Restritiva, disponível em: http://shark.objectweb.org/license.html (http://shark.objectweb.org/license.html).

Esper. Copyright © 2005-2006, Codehaus.

FESI é licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.lugrin.ch/fesi/index.html (http://www.lugrin.ch/fesi/index.html).

jTDS-1.2.2.jar é licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://jtds.sourceforge.net/ (http://jtds.sourceforge.net/).

MDateSelector. Copyright © 2005, Martin Newstead, licenciado sobre a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://web.ukonline.co.uk/mseries (http://web.ukonline.co.uk/mseries).

Tagish Java Authentication and Authorization Service Modules, licenciados sob a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://free.tagish.net/jaas/index.jsp (http://free.tagish.net/jaas/index.jsp).

Este produto pode incluir o software a seguir desenvolvido pela The Apache Software Foundation (http://www.apache.org/ (http://www.apache.org/)) e licenciado sob a Licença do Apache, Versão 2.0 (a "Licença"); o texto da licença pode ser encontrado no diretório Licenses ou em http://www.apache.org/licenses/LICENSE-2.0 (http://www.apache.org/licenses/LICENSE-2.0). A menos que exigido por lei aplicável ou acordado por escrito, o software distribuído sob a Licença é distribuído "NO ESTADO EM QUE SE ENCONTRA", E NÃO OFERECE GARANTIAS OU CONDIÇÕES DE QUALQUER TIPO, sejam elas expressas ou implícitas. Consulte a Licença do idioma específico que governa permissões e limitações sob a Licença.

Apache Axis e Apache Tomcat, Copyright © 1999 a 2005, Apache Software Foundation. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.apache.org/licenses/. (http://www.apache.org/licenses/.)

Apache FOP.jar, Copyright 1999-2007, Apache Software Foundation. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.apache.org/licenses/ (http://www.apache.org/licenses/).

Apache Lucene, Copyright © 1999 a 2005, Apache Software Foundation. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.apache.org/licenses/ (http://www.apache.org/licenses/).

Bean Scripting Framework (BSF), licenciado pela Apache Software Foundation Copyright © 1999-2004. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://xml.apache.org/dist/LICENSE.txt (http://xml.apache.org/dist/LICENSE.txt).

Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licenciado pela Apache Software License. Para obter mais informações, isenções de responsabilidade e restrições, consulte https://skinlf.dev.java.net/ (https://skinlf.dev.java.net/).

Xalan e Xerces, licenciados pela Apache Software Foundation Copyright © 1999-2004. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://xml.apache.org/dist/LICENSE.txt (http://xml.apache.org/dist/LICENSE.txt).

Este produto pode incluir os programas com código-fonte aberto a seguir, disponíveis sob a licença Java.

OBSERVAÇÃO: A partir da publicação desta documentação, os links acima se tornaram ativos. Caso você descubra que alguns links acima foram desfeitos ou que as páginas da Web vinculadas estão inativas, contate a Novell, Inc. no endereço 404 Wyman Street, Suite 500, Waltham, MA 02451 EUA.

Índice

8 Crystal Reports para Windows 97

9 Crystal Reports para Linux 127

Prefácio

O Sentinel™ é uma solução de gerenciamento de eventos e informações de segurança que recebe dados de muitas fontes em toda a empresa e, em seguida, padroniza, prioriza e apresenta esses dados para que você tome decisões relacionadas a ameaças, riscos e políticas.

Público

Essa documentação é destinada aos profissionais de segurança da informação.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no GroupWise. Use a função Comentários do Usuário, situada na parte inferior de cada página da documentação online e digite seus comentários.

Documentação adicional

A documentação técnica do Sentinel está dividida em seis volumes. São eles:

- Guia de Instalação do Sentinel 6.1
- Guia do Usuário do Sentinel 6.1
- Guia de Referência do Usuário do Sentinel 6.1
- A documentação deste produto está disponível em http://www.novell.com/documentation/sentinel6/index.html

Volume I – Guia de Instalação do Sentinel

Este guia explica como instalar os seguintes componentes do Sentinel:

- Servidor de Comunicação do Sentinel
- DAS (Data Access Service - Serviço de Acesso a Dados)
- Sentinel Control Center
- Mecanismo de Correlação do Sentinel
- Gerenciador de Coletor
- Crystal Reports Server
- Advisor
- Construtor de Coletor
- Gerenciador de Dados do Sentinel
- Designer de Soluções do Sentinel

Volume II – Guia do Usuário do Sentinel

Este guia explica como usar os componentes e os recursos do Sentinel:

- Operação do Console do Sentinel
- Recursos do Sentinel
- Arquitetura do Sentinel
- Comunicação do Sentinel
- Encerramento/Inicialização do Sentinel
- Avaliação de vulnerabilidade
- Monitoramento de Eventos
- Filtragem de Eventos
- Correlação de Eventos
- Gerenciador de Dados do Sentinel
- Configuração de Eventos para Relevância Comercial
- Serviço de Mapeamento
- Geração de Relatórios de Histórico
- Gerenciamento de Host do Coletor
- Incidentes
- Casos
- Gerenciamento de Usuário
- Workflow
- Solution Packs

Volume III – Guia do Usuário do Construtor de Coletor

Este guia explica como usar o Construtor de Coletor:

- Operação do Construtor de Coletor
- Gerenciador de Coletor
- Coletores
- Gerenciamento de Host do Coletor
- Construindo e mantendo coletores

Volume IV – Guia de Referência do Usuário do Sentinel

Este guia aborda os seguintes tópicos avançados:

- Linguagem de criação de scripts do coletor
- Comandos de análise do coletor
- Funções de administrador do coletor
- Tags META do Sentinel e do coletor
- Mecanismo de correlação do Sentinel
- Permissões de usuário
- Opções da linha de comando de correlação
- Esquema do banco de dados do Sentinel

Volume V – Guia de Integração de Terceiros do Sentinel

Este guia explica como usar o Sentinel com diversos aplicativos de terceiros:

- Remedy
- HP OpenView Operations
- HP Service Desk

Volume VI - Guia de Instalação de Patch do Sentinel

Este guia explica como fazer o upgrade de uma versão do Sentinel para outra.

- Patches do Sentinel 4.x para o 6.0
- Patches do Sentinel 5.1.3 para o 6.0

Convenções da documentação

Veja a seguir as convenções usadas neste manual:

- Notas e Avisos

Observação: As Notas fornecem informações adicionais que podem ter utilização prática ou podem servir apenas para referência.

Aviso: Os Avisos fornecem informações adicionais que ajudam você a identificar e a interromper ações que possam causar danos ou perda de dados.

- Os comandos aparecem na fonte Courier. Por exemplo:

```
useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
```

- Vá para Iniciar > Arquivos de Programas > Painel de Controle para executar várias ações em uma etapa.
- Referências

  Para obter mais informações, consulte "Nome da Seção" (se estiver no mesmo Capítulo).

  Para obter mais informações, consulte "Nome do Capítulo" (se estiver no mesmo Guia).

  Para obter mais informações, consulte Nome da Seção em Nome do Capítulo, *Nome do Guia* (se estiver em outro Guia).

Na documentação da Novell, o símbolo de maior que (>) é usado para separar as ações de uma etapa e os itens de um caminho de referência cruzada.

Um símbolo de marca registrada (®, ,tm etc.) representa uma marca registrada da novell; o asterisco (*) indica uma marca registrada de terceiros.

Quando for possível digitar um determinado nome de caminho com uma barra invertida em algumas plataformas ou com uma barra regular em outras, o nome do caminho será apresentado com uma barra invertida. Os usuários de plataformas que exigem uma barra regular, como o Linux ou UNIX, devem utilizar barras regulares, de acordo com as exigências do software.

Entrar em Contato com a Novell

- Site na web: http://www.novell.com.br (http://www.novell.com)
- Suporte Técnico da Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Auto-suporte: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site de download de patches: http://download.novell.com/index.jsp (http://download.novell.com/index.jsp)
- Suporte 24 horas: http://www.novell.com/company/contact.html. (http://www.novell.com/company/contact.html.)
- Para Coletores/Conectores/Relatórios/Correlação/Hotfixes/TIDS: http://support.novell.com/products/sentinel (http://support.novell.com/products/sentinel).

Introdução 1

As seções a seguir contêm informações básicas sobre o produto. O restante do *Guia do Usuário do Sentinel* possui procedimentos mais detalhados de administração, operação e arquitetura.

Estas seções supõem que você esteja familiarizado com segurança de rede, administração de bancos de dados e sistemas operacionais Windows* e UNIX*.

1.1 Visão geral do Sentinel

O Sentinel™ é uma solução de gerenciamento de eventos e informações de segurança que recebe dados de muitas fontes em toda a empresa e, em seguida, padroniza, prioriza e apresenta esses dados para que você tome decisões relacionadas a ameaças, riscos e políticas.

O Sentinel automatiza os processos de geração de relatórios, análise e coleta de registros para garantir que os controles de TI sejam eficazes no suporte à detecção de ameaças e aos requisitos de auditoria. O Sentinel substitui esses processos manuais muito trabalhosos por monitoração contínua e automatizada de eventos de conformidade e segurança e controles de TI.

O Sentinel coleta e correlaciona informações de segurança e outros tipos de informação em toda a infra-estrutura de rede da organização, bem como em sistemas, dispositivos e aplicativos de terceiros. O Sentinel apresenta os dados coletados em uma interface gráfica aprimorada, identifica problemas de conformidade ou segurança e monitora atividades de correção, para aperfeiçoar processos sujeitos a erros e construir um programa de gerenciamento mais rigoroso e seguro.

O gerenciamento de respostas a incidentes automatizado permite que você documente e formalize o processo de monitoramento, encaminhamento e resposta a incidentes e violações de política, e fornece uma integração bidirecional com sistemas de comunicação de problemas. O Sentinel permite que você reaja prontamente e resolva incidentes de forma eficiente.

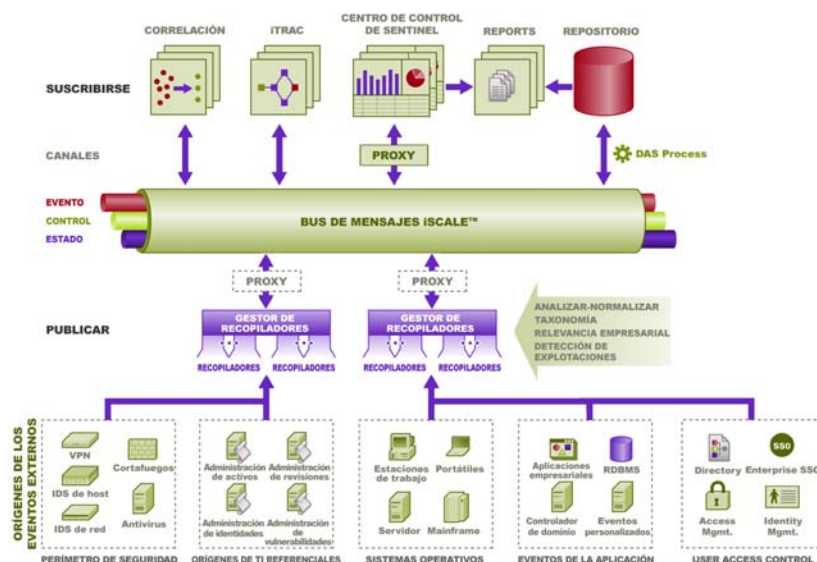
Os Solution Packs são uma maneira simples de distribuir e importar para controles regras de correlação, listas dinâmicas, mapas, relatórios e workflows do iTRAC no Sentinel. Esses controles podem ser criados para atender a requisitos regulatórios específicos, como o Payment Card Industry Data Security Standard, ou podem ser relacionados a uma determinada fonte de dados, como os eventos de autenticação do usuário de um banco de dados Oracle.

O Sentinel oferece o seguinte:

- Gerenciamento de segurança em tempo real automatizado e integrado e monitoração de conformidade entre todos os sistemas e redes.
- Uma estrutura que habilita políticas de negócios para orientar ações e políticas de TI.
- Documentação e relatórios automáticos de segurança, sistemas e eventos de acesso em toda a empresa.

- Gerenciamento de incidentes e correção incorporados.
- A capacidade de demonstrar e monitorar a conformidade com políticas internas e regulamentos governamentais, como Sarbanes-Oxley, HIPAA, GLBA, FISMA e outros. O conteúdo necessário para a implementação desses controles é distribuído e implementado de forma simples por meio dos Solution Packs.

Veja a seguir uma arquitetura conceitual do Sentinel, que ilustra os componentes envolvidos na execução do gerenciamento de segurança e conformidade.

Figura 1-1 *Arquitetura conceitual do Sentinel*

1.2 Interfaces do usuário do Sentinel

O Sentinel contém várias interfaces do usuário fáceis de usar:

- Sentinel Control Center
- Gerenciador de Dados do Sentinel
- Designer de Soluções do Sentinel
- Construtor de Coletor do Sentinel

1.2.1 Sentinel Control Center

O Sentinel Control Center fornece um painel de gerenciamento de segurança integrado que permite que analistas identifiquem rapidamente novas tendências ou ataques, manipulem e interajam com informações gráficas em tempo real e respondam a incidentes. Os recursos principais do Sentinel Control Center incluem:

- **Telas Ativas:** Estatísticas e visualização em tempo real
- **Incidentes:** Criação e gerenciamento de incidentes
- **Correlação:** definição e gerenciamento de regras de correlação
- **iTRAC:** Gerenciamento de processos para a documentação, a imposição e o monitoramento dos processos de resolução de incidentes

- **Gerador de Relatórios:** Métricas e relatórios de histórico
- **Gerenciamento de Fonte de Eventos:** Implantação e monitoração do coletor

1.2.2 Gerenciador de Dados do Sentinel

O Gerenciador de Dados do Sentinel (SDM) permite gerenciar o Banco de Dados do Sentinel. Você pode executar as seguintes operações no SDM:

- Monitorar a utilização de espaço do banco de dados
- Ver e gerenciar as partições de banco de dados
- Gerenciar arquivos de bancos de dados
- Importar dados para o banco de dados

1.2.3 Designer de Soluções do Sentinel

O Designer de Soluções do Sentinel é usado para criar e modificar Solution Packs, que são conjuntos de conteúdo do Sentinel agrupados em pacotes, como relatórios, regras de correlação e workflows.

1.2.4 Construtor de Coletor do Sentinel

O Construtor de Coletor do Sentinel permite que você crie Coletores no idioma proprietário do Sentinel para processar eventos. Você pode criar e personalizar os gabaritos para que o Coletor possa analisar os dados.

1.3 Componentes do Sentinel Server

O Sentinel é formado por vários componentes:

- DAS (Data Access Service - Serviço de Acesso a Dados)
- Servidor de Comunicação do Sentinel
- Banco de Dados do Sentinel
- Gerenciador de Coletor do Sentinel
- Mecanismo de Correlação
- iTRAC™
- Crystal Reports Server *
- Sentinel Advisor e Detecção de Exploração (opcional)

1.3.1 Sentinel Server

O DAS (Serviço de Acesso a Dados) é o principal componente usado na comunicação com o banco de dados do Sentinel. O DAS e outros componentes do servidor trabalham juntos para armazenar eventos recebidos dos Gerenciadores de Coletor no banco de dados, filtrar dados, processar exibições de Tela Ativa, executar consultas de bancos de dados e processar resultados, e também gerenciar tarefas administrativas, como autorização e autenticação do usuário.

1.3.2 Servidor de Comunicação do Sentinel

O Barramento de Mensagem iSCALE™ pode mover milhares de pacotes de mensagens em um segundo entre os componentes do Sentinel. Isso permite o dimensionamento independente dos componentes e a integração baseada em padrões com aplicativos externos.

1.3.3 Banco de Dados do Sentinel

O Sentinel tem como base um banco de dados de back end que armazena eventos de segurança e todos os metadados do Sentinel. Os eventos são armazenados em formato normalizado juntamente com dados de vulnerabilidade e bens, informações de identidade, status de incidente e workflow e muitos outros tipos de dados.

1.3.4 Gerenciador de Coletor do Sentinel

O Gerenciador de Coletor gerencia a coleta de dados, monitora as mensagens de status do sistema e executa a filtragem de eventos conforme necessário. As principais funções do Gerenciador de Coletor incluem transformar eventos, adicionar relevância comercial aos eventos por meio de taxonomia, executar filtragem global nos eventos, rotear eventos e enviar mensagens sobre saúde ao Sentinel Server.

O Gerenciador de Coletor do Sentinel pode se conectar diretamente ao barramento de mensagem ou usar um proxy SSL.

1.3.5 Mecanismo de Correlação

A correlação agrega inteligência ao gerenciamento de eventos de segurança automatizando a análise do fluxo de eventos de entrada para encontrar padrões relevantes. A correlação permite definir regras que identificam as ameaças importantes e padrões complexos de ataque, para que você consiga priorizar os eventos e iniciar o gerenciamento e a resposta eficazes aos incidentes.

1.3.6 iTRAC

O Sentinel fornece um sistema de gerenciamento de workflow do iTRAC para que você possa definir e automatizar processos de respostas a incidentes. Incidentes identificados no Sentinel, seja por uma regra de correlação ou manualmente, podem ser associados a um workflow do iTRAC.

1.3.7 Crystal Reports Server

Serviços de geração de relatórios abrangentes do Sentinel Control Center são fornecidos pelo Crystal Reports Server da Business Objects*. O Sentinel é fornecido com relatórios predefinidos direcionados às solicitações de relatórios mais comuns de organizações que monitoram suas posturas de segurança e conformidade. Usando o Crystal Reports Developer, você também poderá desenvolver relatórios novos ou personalizados de acordo com o esquema de tela de relatório publicado do Sentinel.

1.3.8 Sentinel Advisor e Detecção de Exploração

O Sentinel Advisor é um serviço opcional de inscrição de dados que inclui informações sobre ataques conhecidos, vulnerabilidades e correções. Esses dados, combinados com informações sobre vulnerabilidades conhecidas e sobre prevenção ou detecção de intrusão em tempo real no ambiente, fornecem uma detecção de exploração proativa e a capacidade de agir imediatamente quando um ataque ocorre em um sistema vulnerável.

1.4 Plug-ins do Sentinel

O Sentinel suporta vários plug-ins, o que permite expandir e aprimorar a funcionalidade do sistema. Alguns desses plug-ins são instalados automaticamente. Plug-ins (e atualizações) adicionais estão disponíveis para download em http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html).

Alguns plug-ins, como o Remedy* Integrator e o IBM* Mainframe Connector, exigem uma licença adicional para download.

1.4.1 Coletores

O Sentinel coleta dados em dispositivos de origem e distribui um fluxo de eventos enriquecido aplicando taxonomia, detecção de exploração e relevância comercial ao fluxo de dados antes que os eventos sejam correlacionados, analisados e enviados para o banco de dados. Um fluxo de eventos enriquecido significa que os dados estão correlacionados ao contexto comercial necessário para identificar e resolver ameaças internas ou externas e violações às políticas.

Os Coletores do Sentinel podem analisar dados dos tipos de dispositivos listados abaixo:

- Sistemas de detecção de intrusão (host)
- Sistemas de detecção de intrusão (rede)
- Firewalls.
- Sistemas Operacionais
- Monitoramento de políticas
- Autenticação
- Roteadores e switches
- VPNs
- Sistemas de detecção antivírus
- Servidores da Web
- Bancos de Dados
- Mainframe
- Sistemas de avaliação de vulnerabilidade
- NDS
- Sistemas de gerenciamento de redes
- Sistemas proprietários

Os Coletores do JavaScript podem ser criados e executados no Sentinel 6.0 SP1 e em versões posteriores por meio de ferramentas de desenvolvimento padrão do JavaScript e do SDK do Coletor. Os Coletores proprietários podem ser construídos ou modificados no Seção 1.2.4, “Construtor de Coletor do Sentinel” na página 15, um aplicativo independente incluído no sistema Sentinel.

1.4.2 Conectores e integradores

Os conectores fornecem conectividade entre o Gerenciador de Coletor e fontes de eventos por meio de protocolos padrão como JDBC e syslog. Os eventos são passados do Conector ao Coletor para análise.

Os integradores permitem a execução de ações de correção em sistemas situados fora do Sentinel. Por exemplo, uma ação de correlação pode usar o Integrador SOAP para iniciar um workflow do Novell Identity Manager.

O Remedy AR Integrator opcional permite criar um ticket de correção a partir de incidentes ou eventos do Sentinel.

1.4.3 Ações e regras de correlação

As regras de correlação identificam padrões importantes no fluxo de eventos. Quando acionada, a regra de correlação inicia ações de correlação, como o envio de notificações por e-mail, a inicialização de um workflow do iTRAC ou a execução de uma ação por meio de um Integrador.

1.4.4 Relatórios

Os usuários podem executar uma grande variedade de relatórios operacionais e de painel no Sentinel Control Center usando o Crystal Reports Server. Geralmente, no Sentinel 6.1 e em versões posteriores, os relatórios são distribuídos por meio de Solution Packs.

1.4.5 Workflows do iTRAC

Os workflows do iTRAC fornecem processos consistentes e reutilizáveis para o gerenciamento de incidentes. Geralmente, no Sentinel 6.1 e em versões posteriores, os gabaritos de workflow são distribuídos por meio de Solution Packs.

1.4.6 Solution Packs

Os Solution Packs são pacotes de conteúdo relacionado do Sentinel, como regras de correlação, ações, worflows do iTRAC e relatórios. A Novell fornece Solution Packs destinados a necessidades comerciais específicas, como o Solution Pack PCI-DSS, que aborda a conformidade com o Payment Card Industry Data Security Standard. Além disso, a Novell cria “collector packs,” que incluem conteúdo concentrado em uma fonte de eventos específica, como o Windows Active Directory.

1.5 Suporte a idiomas

Os componentes do Sentinel foram traduzidos para os seguintes idiomas:

- Inglês
- Português (Brasil)
- Francês
- Italiano
- Alemão
- Espanhol
- Japonês
- Chinês (Tradicional)
- Chinês (Simplificado)

Há várias exceções:

- A interface do Construtor de Coletor e a criação de scripts estão somente em inglês, embora possam ser executadas em sistemas operacionais nos outros idiomas listados acima.
- Os Coletores do JavaScript podem ser modificados para analisar dados ASCII ou Unicode (byte duplo), mas os Coletores publicados no site de Conteúdo do Sentinel só estão disponíveis em inglês. Os Coletores escritos no idioma proprietário só podem processar dados ASCII e ASCII estendidos.
- Eventos internos (para auditar operações do Sentinel) só estão disponíveis em inglês.

Requisitos do sistema

2

2.1 Software suportado

Para a obtenção de bom desempenho e confiabilidade, a Novell recomenda que os clientes instalem todos os componentes do Sentinel em softwares aprovados, como os listados a seguir, que tenham passado por certificação e controle de qualidade completos. Para obter as informações mais recentes sobre os requisitos mínimos, procure atualizações no site de Documentação da Novell (http://www.novell.com/documentation/sentinel61).

A tabela a seguir lista os níveis de patch específicos usados na realização do teste do Sentinel. Por conveniência, neste documento as plataformas serão mencionadas por seus nomes abreviados, localizados na coluna da esquerda. Em situações em que o comprimento de bit for irrelevante, ele poderá aparecer truncado no nome abreviado.

Tabela 2-1 *Informações de nível de patch*

Nome abreviado	Nome completo e nível de patch
SLES 10 (32 bits)	SUSE® Linux Enterprise Server 10 SP1 (32 bits)
SLES 10 (64 bits)	SUSE Linux Enterprise Server 10 SP1 (64 bits)
RHEL 4 (32 bits)	Red Hat Enterprise Linux 4 Nahant Update-4 (32 bits)
RHEL 4 (64 bits)	Red Hat Enterprise Linux 4 Nahant Update-4 (64 bits)
Solaris 10 (64 bits)	Sun Solaris 10 6/06 s10s_u2wos_09a (SPARC de 64 bits)
Windows 2003 (32 bits)	Windows 2003 SP2, Standard ou Enterprise Edition (32 bits)
Windows 2003 (64 bits)	Windows 2003 SP1, Standard ou Enterprise Edition (64 bits)
Windows 2008 (De 64 bits)	Windows 2008 SP1, Standard Edition (64 bits)
SLED 10 (De 32 bits)	SUSE® Linux Enterprise Desktop 10 SP1 (32 bits)
Windows XP (32 bits)	Windows XP SP2 (32 bits)
Windows Vista (De 32 bits)	Windows Vista SP1 (32 bits)
Oracle 10 (32 bits)	Oracle* 10g Enterprise Edition com particionamento (v 10.2.0.3 - 5901891 inclui patch crítico #5881721, patch de segurança 6864068) (32 bits), executado no SuSE Linux Enterprise Server 10 (32 bits)
Oracle 10 (64 bits)	Oracle 10g Enterprise Edition com particionamento (v 10.2.0.3 - 5901891 inclui patch crítico #5881721, patch de segurança 6864068), executado em (64 bits)
SQL Server 2005 (32 bits)	Microsoft SQL Server 2005 SP2, Standard ou Enterprise Edition (32 bits)

Nome abreviado	Nome completo e nível de patch
SQL Server 2005 (64 bits)	Microsoft SQL Server 2005 SP2, Standard ou Enterprise Edition (64 bits)
SQL Server 2008 (De 64 bits)	Microsoft SQL Server 2008 CTP Fevereiro de 2008 (64 bits)
SLES 9 (De 32 bits)	SuSE Linux Enterprise Server 9 SP2 (32 bits)

Consulte os respectivos fornecedores para obter patches e atualizações de segurança. Geralmente, esses hotfixes e patches de segurança não afetam as operações do Sentinel e, portanto, são suportados. Como lançamentos de maior ou menor importância de um banco de dados ou de um sistema operacional quase sempre envolvem mudanças significativas, apenas as versões mencionadas acima são suportadas para este lançamento.

2.1.1 Plataformas de banco de dados suportadas

As combinações de bancos de dados e sistemas operacionais a seguir são marcadas como certificadas ou suportadas. As combinações certificadas foram testadas com o suíte de teste completo do Novell Engineering. As combinações suportadas devem ser totalmente funcionais.

Tabela 2-2 *Plataformas de banco de dados suportadas*

	Oracle 10 (32)	Oracle 10 (64)	SQL Server 2005 (32)	SQL Server 2005 (64)	MS SQL 2008 (64)
SLES 10 (32)	Suportado	Não suportado	Não suportado	Não suportado	Não suportado
SLES 10 (64)	Não suportado	Certificado	Não suportado	Não suportado	Não suportado
RHEL 4 (32)	Suportado	Não suportado	Não suportado	Não suportado	Não suportado
RHEL 4 (64)	Não suportado	Suportado	Não suportado	Não suportado	Não suportado
Solaris 10 (32)	Suportado	Não suportado	Não suportado	Não suportado	Não suportado
Solaris 10 (64)	Não suportado	Suportado	Não suportado	Não suportado	Não suportado
Windows 2003 (32)	Não suportado	Não suportado	Suportado	Não suportado	Não suportado
Windows 2003 (64)	Não suportado	Não suportado	Não suportado	Certificado	Não suportado
Windows 2008 (64)	Não suportado	Não suportado	Não suportado	Não suportado	Suportado

Embora plataformas de 32 bits sejam suportadas para o banco de dados do Sentinel em ambientes de desenvolvimento ou de prova de conceito, para que os melhores resultados de desempenho sejam obtidos, a Novell recomenda plataformas de 64 bits para bancos de dados de produção.

O Sentinel foi testado com a versão beta do Microsoft SQL Server 2008 CTP Fevereiro de 2008 (64 bits). Não havia nenhum erro conhecido no momento da publicação, mas qualquer mudança feita no banco de dados antes do lançamento oficial poderá afetar as operações do Sentinel.

Observação: Para serem usados com componentes do Sentinel, todos os bancos de dados devem estar instalados em um sistema operacional certificado pelo fornecedor do banco de dados e também pela Novell. O Oracle deve ser executado no Linux* ou no Solaris (não no Windows).

2.1.2 Componentes do Sentinel

Os componentes do Sentinel Server incluem o Servidor de Comunicação, o Mecanismo de Correlação, o DAS (Serviço de Acesso a Dados) e o serviço de inscrição de dados do Advisor (que reside na mesma máquina que o DAS).

Os Aplicativos de Usuário do Sentinel contidos na tabela a seguir incluem o Sentinel Control Center, o Gerenciador de Dados do Sentinel e o Designer de Soluções do Sentinel.

O Gerenciador de Coletor, o Construtor de Coletor e o Crystal Reports Server também possuem requisitos de plataforma específicos.

As combinações de softwares e sistemas operacionais a seguir são marcadas como certificadas (C) ou suportadas (S). As combinações certificadas foram testadas com o suíte de teste completo do Novell Engineering. As combinações suportadas devem ser totalmente funcionais.

Tabela 2-3 *Combinações de softwares e sistemas operacionais*

	Componentes do Sentinel Server	Aplicativos de Usuário do Sentinel	Gerenciador de Coletor	Construtor de Coletor	Crystal Reports Server
SLES 10 (32)	Suportado	Suportado	Certificado	Não suportado	Não suportado
SLES 10 (64)	Certificado	Suportado	Suportado	Não suportado	Não suportado
RHEL 4 (32)	Suportado	Suportado	Suportado	Não suportado	Certificado
RHEL 4 (64)	Suportado	Suportado	Suportado	Não suportado	Não suportado
Solaris 10 (32)	Suportado	Suportado	Certificado	Não suportado	Não suportado
Solaris 10 (64)	Certificado	Suportado	Suportado	Não suportado	Não suportado
Windows 2003 (32)	Suportado	Suportado	Certificado	Suportado	Certificado
Windows 2003 (64)	Certificado	Suportado	Suportado	Suportado	Não suportado
Windows 2008 (64)	Suportado	Suportado	Suportado	Suportado	Não suportado
SLED 10	Não suportado	Certificado	Não suportado	Não suportado	Não suportado
Windows XP	Não suportado	Certificado	Não suportado	Suportado	Não suportado
Windows Vista	Não suportado	Suportado	Não suportado	Suportado	Não suportado
SLES 9 (32)	Não suportado	Não suportado	Não suportado	Não suportado	Certificado

O servidor de geração de relatórios suportado é o Crystal Reports Server XI R2. O Crystal requer um servidor web e um banco de dados do Servidor de Gerenciamento Central (CMS) para funcionar, além do banco de dados do Sentinel. O Crystal Reports Server pode ser executado nas seguintes plataformas do ambiente do Sentinel:

- Red Hat Enterprise Linux 4 (32 bits)
  - Banco de dados do CMS do Crystal no MySQL
  - Servidor web no Apache Tomcat
  - É recomendável usar o banco de dados do Sentinel no Oracle; não foram testadas outras configurações
- SuSE Linux Enterprise Server 9 SP2 (32 bits)
  - Banco de dados do CMS do Crystal no MySQL
  - Servidor web no Apache Tomcat
  - É recomendável usar o banco de dados do Sentinel no Oracle; não foram testadas outras configurações
- Windows 2003 SP1 Server, Standard ou Enterprise Edition (32 bits)
  - Banco de dados do CMS do Crystal no Microsoft SQL Server 2005
  - Servidor web no Microsoft IIS com .NET
  - É recomendável usar o banco de dados do Sentinel no SQL Server; não foram testadas outras configurações

A Novell testou a publicação e a execução de relatórios na interface do Sentinel usando as seguintes versões do Crystal:

- **No Linux:** Crystal Reports Server XI R2 SP2
- **No Windows:** Crystal Reports Server XI R2 SP3

É possível fazer download desses service packs na seção Download do site da SAP na web, no endereço

https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads)

Consulte a documentação do fornecedor para obter detalhes adicionais sobre os requisitos do sistema, os números de versão suportados e os problemas conhecidos das plataformas.

2.1.3 Avisos de cuidado e exceções de suporte a plataformas

As seguintes plataformas não são suportadas por seus respectivos fornecedores e, portanto, também não serão suportadas pela Novell:

- Atualmente, o fornecedor do Crystal Reports Server XI R2 não suporta o Crystal no Solaris nem no SUSE Linux Enterprise Server 10; portanto, a Novell também não suporta essas combinações.
- Atualmente, a Oracle não suporta o Oracle 10 (32 bits) no Solaris 10 de 32 bits

Embora as configurações de plataforma a seguir possam ser suportadas por seus respectivos fornecedores, a Novell não recomenda o uso dessas configurações em um ambiente do Sentinel:

- Sentinel no SUSE Linux Enterprise Server 10 executado com o sistema de arquivos ReiserFS
- Banco de dados Oracle no Microsoft Windows
- Crystal Reports Server no Microsoft Windows 2000
- Crystal Reports Server com MSDE como banco de dados

Embora a Novell recomende que o banco de dados do Sentinel e o mecanismo gerador de relatórios sejam executados em plataformas que tenham passado pelo controle de qualidade completo da Novell, tanto o banco de dados Oracle quanto o Crystal Reports Server são suportados em plataformas adicionais por seus respectivos fornecedores. Se um cliente desejar usar uma dessas plataformas adicionais, a Novell fornecerá algum suporte, com exceções.

- Como a instalação e a configuração do banco de dados do Sentinel são processos específicos da plataforma, é recomendável utilizar a consultoria da Novell ou um parceiro qualificado ao instalar e configurar o Sentinel pela primeira vez.
- O instalador padrão pode não funcionar conforme o esperado em uma plataforma não testada.
- Quando o sistema Sentinel estiver funcionando, todos os problemas de geração de relatórios ou de banco de dados que não puderem ser reproduzidos internamente nas plataformas suportadas deverão ser solucionados pelo fornecedor apropriado.

Por fim, para que a funcionalidade total seja obtida, a Novell recomenda que o banco de dados e o DAS sejam instalados com o mesmo sistema operacional (embora não necessariamente na mesma máquina). (Por exemplo, a Autenticação do Windows não poderá ser usada se o DAS estiver instalado em um ambiente misto em que o DAS esteja no Windows e o banco de dados seja Oracle ou em que o DAS esteja no UNIX ou no Linux e o banco de dados seja SQL Server.)

O Construtor de Coletor só pode ser executado em plataformas Windows.

2.2 Recomendações de hardware

Quando você realiza a instalação no Linux ou no Windows, os componentes do banco de dados e o servidor Sentinel podem ser executados em hardware x86 (32 bits) ou x86-64 (64 bits), com algumas exceções baseadas no sistema operacional, conforme descrito anteriormente. O Sentinel é certificado em hardware AMD Opteron e Intel Xeon. Servidores Itanium não são suportados.

Para Solaris, a arquitetura SPARC é suportada.

Aviso: Devido à natureza de alto desempenho do Sentinel, a Novell recomenda que ele seja executado em hardware dedicado situado em ambientes de produção, e não em Máquinas Virtuais (VMs).

2.2.1 Arquitetura

O Sentinel tem uma arquitetura altamente escalável e, se altas taxas de eventos forem esperadas, os componentes poderão ser distribuídos por várias máquinas para que o melhor desempenho do sistema seja atingido.

Há muitos fatores que você deve levar em consideração ao criar um sistema Sentinel. Veja a seguir uma lista parcial dos fatores que devem ser levados em consideração para o desenvolvimento de um design:

- Taxa de eventos (eventos por segundo ou EPS)
- Localização geográfica/de rede de fontes de eventos e largura de banda entre redes
- Hardware disponível
- Sistemas operacionais preferenciais
- Planos para escalabilidade futura
- Quantidade de filtragem de eventos esperada
- Políticas de retenção de dados locais
- Número e complexidade desejados de regras de correlação
- Número esperado de incidentes por dia
- Número esperado de workflows gerenciados por dia
- Número de usuários conectados ao sistema
- Vulnerabilidade e infra-estrutura de bens

O fator mais significativo no design do sistema Sentinel é a taxa de eventos; quase todos os componentes da arquitetura do Sentinel serão afetados pelo aumento das taxas de eventos. Em um ambiente com alta taxa de eventos, a maior demanda recairá sobre o banco de dados, que é muito dependente da E/S e poderá estar processando simultaneamente inserções de centenas ou milhares de eventos por segundo, criações de objetos por vários usuários, atualizações de processos de workflow, consultas simples de histórico no Sentinel Control Center e relatórios de longo prazo do Crystal Enterprise Server. Portanto, a Novell faz as seguintes recomendações:

- O banco de dados deve ser instalado sem nenhum outro componente do Sentinel.
- O servidor do banco de dados deve ser dedicado às operações do Sentinel. Processos de aplicativos adicionais ou ETL (Extract Transform Load) podem afetar o desempenho do banco de dados.
- O servidor do banco de dados deve ter uma matriz de armazenamento de alta velocidade que atenda aos requisitos de E/S com base nas taxas de inserção de eventos.
- O Administrador do Banco de Dados dedicado deve fazer regularmente a avaliação e a manutenção dos seguintes aspectos do banco de dados:
  - Tamanho
  - Operações de E/S
  - Espaço em disco
  - Memória
  - Indexação
  - Registros de transação

Em ambientes de baixa taxa de eventos (por exemplo, eps < 25), as recomendações fornecidas acima não precisam ser seguidas, pois o banco de dados e os outros componentes usam menos recursos.

Esta seção contém algumas recomendações gerais sobre hardware que poderão orientar você em relação ao design do sistema Sentinel. Em geral, as recomendações de design são baseadas em faixas de taxas de eventos. No entanto, essas recomendações são baseadas nas seguintes suposições:

- A taxa de eventos está na extremidade alta da faixa de EPS.
- A média de tamanho dos eventos é 600 bytes.
- Todos eventos são armazenados no banco de dados (isto é, não há filtros para descartar eventos).
- Um volume de dados de trinta dias será armazenado online no banco de dados.
- O espaço de armazenamento para os dados do Advisor não está incluído nas especificações contidas nas tabelas abaixo.
- Por padrão, o Sentinel Server possui 5 GB de espaço em disco para armazenar em cache temporariamente os dados de eventos não inseridos no banco de dados.
- O Sentinel Server também possui por padrão 5 GB de espaço em disco para eventos que não são gravados nos arquivos de eventos de agregação.

Observação: A inscrição opcional do Advisor requer 50 GB adicionais de espaço em disco no servidor de banco de dados.

As recomendações de hardware para uma implementação do Sentinel podem variar de acordo com a implementação; portanto, é recomendável que você consulte o Novell Consulting Services antes de finalizar a arquitetura do Sentinel. As recomendações a seguir podem ser usadas como diretrizes.

Observação: Devido às altas cargas de eventos e ao cache local, a máquina do Sentinel Server com o DAS (Serviço de Acesso a Dados) precisa ter uma matriz de disco distribuída local ou compartilhada (RAID) com no mínimo 4 eixos de disco.

Os hosts distribuídos devem ser conectados aos outros hosts do Sentinel Server por meio de um switch único de alta velocidade (GIGE) para impedir gargalos de tráfego de rede.

A Novell recomenda que o Crystal Reports Server seja instalado em uma máquina dedicada, especialmente se o banco de dados for grande ou se o uso de relatórios for intenso. O Crystal poderá ser instalado na mesma máquina que o banco de dados se o banco de dados for pequeno, se o gerador de relatórios não for muito usado e se o banco de dados estiver instalado no Windows ou no Linux (não no Solaris). As configurações sugeridas a seguir representam implementações pequenas, médias e grandes, mas são baseadas no Sentinel 5.1.3. Recomendações atualizadas serão publicadas no Site de Documentação da Novell, localizado em http://www.novell.com/documentation/sentinel61 (http://www.novell.com/documentation/sentinel61), quando o teste for concluído.

Tabela 2-4 Configuração de duas máquinas, usada para 1-500 EPS

1-500 EPS: Configuração de duas máquinas			
Componentes	**RAM**	**Espaço em disco**	**CPU**
Máquina 1: Sentinel Server/ Gerenciador de Coletor ◆ Mecanismo de Correlação ◆ DAS ◆ Servidor de Comunicação ◆ Advisor ◆ Gerenciador de Coletor/ Coletores ◆ Banco de Dados ◆ Crystal Reports Server (opcional para Windows/ Linux)	6 GB	300 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5150 (2,66 GHz) ou Sun Solaris - 4 x UltraSPARC IIIi (1,5 GHz)
Máquina 2: Report Server ◆ Crystal Reports Server	2 GB	20 GB	Windows ou Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

Tabela 2-5 Configuração de três máquinas, usada para 500-1500 EPS

500 – 1500 EPS: Configuração de três máquinas			
Componentes	**RAM**	**Espaço em disco**	**CPU**
Máquina 1: Sentinel Server/Gerenciador de Coletor ◆ Mecanismo de Correlação ◆ DAS ◆ Servidor de Comunicação ◆ Advisor ◆ Gerenciador de Coletor/Coletores	4 GB	90 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Máquina 2: Banco de dados ◆ Banco de Dados ◆ Crystal Reports Server (opcional para Windows/Linux)	4 GB+	1 TB+	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 3: Report Server (necessário somente se o Sentinel/BD estiver instalado no Solaris) ◆ Crystal Reports Server	2 GB	20 GB	Windows ou Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

Tabela 2-6 Configuração de 4 ou 5 máquinas, usada para 1500-3000 EPS

1500 - 3000 EPS: Configuração de 4 ou 5 máquinas			
Componentes	**RAM**	**Espaço em disco**	**CPU**
Máquina 1: Sentinel Server ◆ Mecanismo de Correlação ◆ DAS ◆ Servidor de Comunicação ◆ Advisor	4 GB	90 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Máquina 2: Banco de dados ◆ Banco de Dados ◆ Crystal Reports Server (opcional para Windows/Linux)	8 GB+	3 TB+	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 3: Gerenciador de Coletor ◆ Gerenciador de Coletor/Coletores	2 GB	20 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 4: Report Server ◆ Crystal Reports Server	4 GB	20 GB	Windows ou Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)
Máquina 5: Instância adicional de DAS_Binary (necessário se EPS > 2000) Para obter instruções de configuração, consulte Capítulo 6, “Adicionando componentes do Sentinel” na página 83.	2 GB	40 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+

Instalando o Sentinel 6.1

3

3.1 Visão geral do instalador

Esta seção ajudará você a instalar os principais componentes do sistema Sentinel. O instalador do Sentinel oferece duas opções de instalação: Simples ou Personalizada. A instalação Simples instala todos os componentes em uma máquina e é destinada a sistemas de treinamento ou demonstração. Na instalação Simples, muitas configurações padrão mínimas são usadas e, portanto, ela não deve ser usada para produção. A instalação Personalizada pode ser usada para instalar um ou mais componentes do Sentinel de uma só vez e também para realizar instalações de produção distribuídas.

Além dos componentes do Sentinel, há vários outros aplicativos que podem fazer parte do sistema Sentinel:

- **Banco de Dados:** O banco de dados, que armazena eventos, eventos correlacionados e informações de configuração, é uma parte essencial do sistema Sentinel. O banco de dados deve ser instalado de acordo com as melhores práticas recomendadas pela Oracle e pela Microsoft para instalação de bancos de dados, estrutura de diretórios, etc.
- **Crystal Reports Server:** O Crystal (bem como o banco de dados e o servidor web associados) é usado para executar relatórios da biblioteca de relatórios da Novell ou relatórios personalizados. Existe um instalador separado para os componentes do Crystal. Para obter mais informações sobre a instalação do Crystal, consulte as seções Capítulo 8, "Crystal Reports para Windows" na página 97 e Capítulo 9, "Crystal Reports para Linux" na página 127.
- **Crystal Reports Developer:** Esse aplicativo é usado para criar e modificar relatórios.
- **Advisor:** O Advisor fornece inteligência em tempo real sobre ataques e vulnerabilidades, incluindo detecção de exploração em tempo real para determinar que ameaças estão ocorrendo em sistemas vulneráveis. Esse módulo é opcional. Para obter mais informações sobre o Advisor e sobre o instalador do instantâneo de dados básicos do Advisor, consulte o Capítulo 4, "Configuração do Advisor" na página 63.
- **Integração com Terceiros:** O Sentinel se integra ao HP OpenView Service Desk.

Observação: A integração com o Remedy Service Desk estava disponível anteriormente como opção do instalador. Na versão Sentinel 6.1, a integração com o Remedy é obtida por meio de um plug-in do integrador e não está mais incluída no instalador do Sentinel. Com a licença adequada, o Remedy

Integrator e a Ação associada podem ser transferidos por download do site de conteúdo localizado em http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html).

3.2 Configurações do Sentinel

Veja a seguir algumas configurações comuns do Sentinel. No Linux

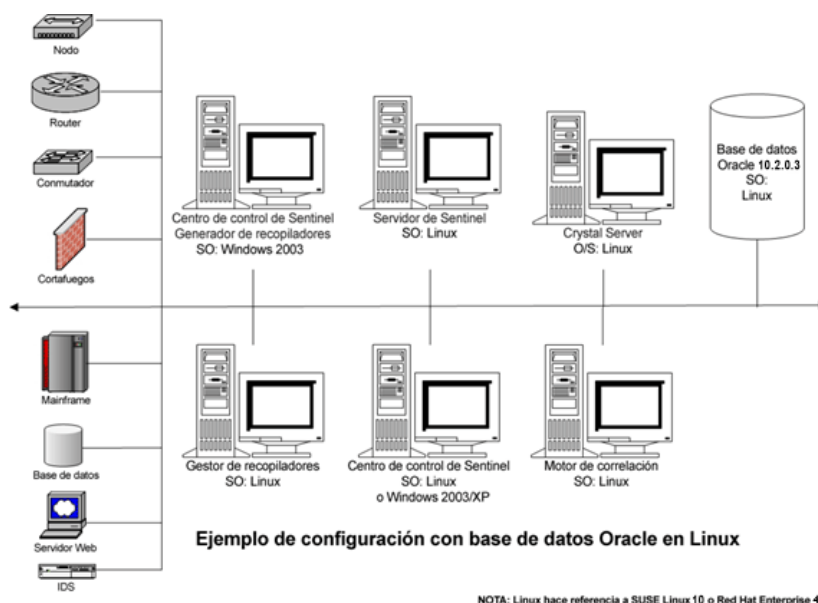
Figura 3-1 Configuração do Sentinel no Linux

3.2.1 No Solaris

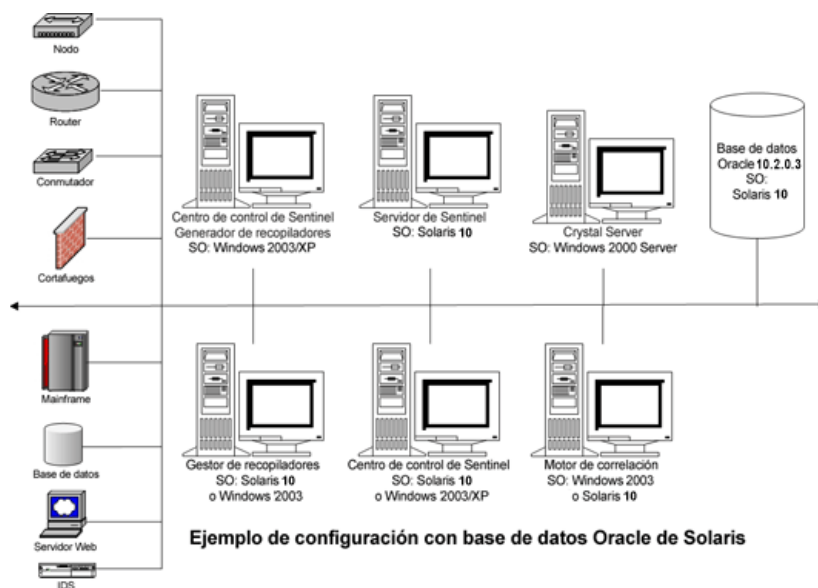
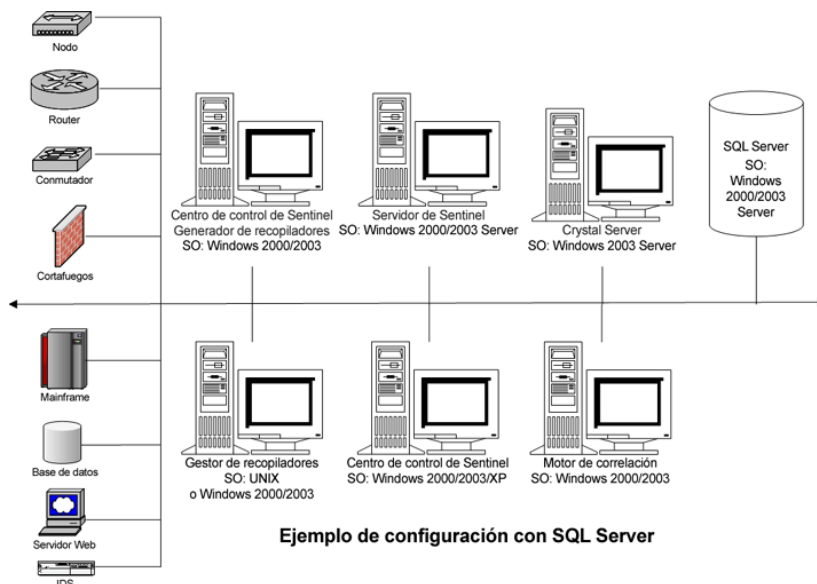
Figura 3-2 Configuração do Sentinel no Solaris

3.2.2 No Windows

***Figura 3-3** Configuração do Sentinel no Windows*

3.3 Pré-requisitos gerais de instalação

Veja a seguir que etapas você deve executar antes de instalar o Sentinel. Para obter mais informações sobre muitos desses pré-requisitos (incluindo a lista de plataformas certificadas), consulte o Capítulo 2, “Requisitos do sistema” na página 21.

- Verifique se todas as máquinas da arquitetura do Sentinel atendem aos requisitos mínimos do sistema.
- Verifique se os sistemas operacionais de todos os componentes do sistema são plataformas certificadas e se foram "protegidos" com a utilização das práticas de segurança recomendadas.
- Se estiver instalando no SUSE Linux Enterprise Server 10, verifique se o SLES está usando o sistema de arquivos ext3.
- Se estiver instalando o Gerenciador de Coletor em uma máquina de 64 bits, verifique se as bibliotecas de 32 bits estão disponíveis. As bibliotecas de 32 bits são necessárias quando você executa um Coletor criado em seu idioma proprietário (que inclui quase todos os Coletores criados antes de junho de 2008), e também quando você executa determinados Conectores (como o Conector LEA). Coletores baseados em JavaScript e o restante do Sentinel são habilitados para 64 bits. Verificar se essas bibliotecas estão disponíveis é muito importante em plataformas Linux, que podem não as incluir por padrão.
- Você deve instalar o pacote SUNWxcu4 na máquina Solaris antes de instalar o Sentinel 6.1.
- Verifique se há um banco de dados certificado para Sentinel instalado. Se estiver usando o Oracle, você precisará ter o Enterprise Edition com particionamento para que o arquivamento dos dados funcione. Para obter mais informações sobre versões certificadas, consulte o Capítulo 2, “Requisitos do sistema” na página 21.

- Obtenha os números de série e as chaves de licença do Sentinel, do Crystal Reports Server e do Crystal Reports Developer no Novell Customer Center (https://secure-www.novell.com/center/regadmin). Se tiver adquirido a alimentação de dados de detecção de exploração opcional do Advisor, verifique no Customer Center se a inscrição desses dados está listada com o resto dos produtos da Novell.
- Instale e configure um servidor SMTP se desejar ter acesso ao recurso de enviar notificações por e-mail a partir do sistema Sentinel.
- Crie um diretório só com caracteres ASCII (sem caracteres especiais) para executar o instalador.
- Forneça privilégios de usuário avançado ao "Usuário de Domínio".

As instalações do Sentinel que usam o instalador completo devem ser sempre realizadas em um sistema "limpo". Se o Sentinel 6 tiver sido instalado anteriormente em alguma das máquinas, a Novell recomenda que você siga os procedimentos de desinstalação no Capítulo 10, "Desinstalando o Sentinel" na página 143. Para obter informações sobre como desinstalar versões anteriores do Sentinel, consulte os guias de instalação relevantes no site de Documentação da Novell (http://www.novell.com/documentation/).

Observação: O instalador de patches contém instruções para o upgrade de uma versão anterior do Sentinel 6 para o Sentinel 6.1.

3.3.1 Fornecendo privilégios de usuário avançado a "Usuários de Domínio"

Importante: Se você instalar o Sentinel como usuário de domínio, em que o usuário não faz parte do grupo de administradores da máquina que contém o diretório ativo e da máquina local, o usuário de domínio deverá ser um usuário avançado para iniciar o Sentinel Services.

Para fornecer privilégios de usuário avançado a usuários de domínio:

1. Clique o botão direito do mouse em Meu Computador e selecione Gerenciar.
2. Na janela Gerenciamento do Computador, selecione Local > Usuários e Grupos > Grupos.
3. Clique duas vezes em Usuário Avançado e adicione o usuário de domínio no formato "domínio/usuário de domínio" ao sistema local em que o Sentinel está instalado usando esse usuário de domínio.

3.3.2 Pré-requisitos de instalação do Banco de Dados do Sentinel

Antes de instalar os componentes do Banco de Dados do Sentinel, você deverá executar as etapas e reunir as informações a seguir.

Pré-requisitos de instalação de banco de dados do Linux/Solaris para o Sentinel

- Se você estiver realizando a instalação no SLES 10, o sistema de arquivos do sistema operacional deverá ser ext3.
- No Linux/Solaris, o banco de dados Oracle deve estar instalado e em execução.

- No Linux/Solaris, o cliente JDBC Oracle (`ojdbc14.jar`) deve estar instalado na máquina em que o instalador está sendo executado. Se você executar o instalador do Sentinel na máquina que possui o banco de dados, um cliente JDBC compatível já deverá ter sido instalado pelo instalador do banco de dados. Se você executar o instalador do Sentinel em outra máquina, a instância de banco de dados deverá ser criada manualmente e o cliente JDBC compatível deverá ser instalado manualmente na máquina com o instalador. Embora os drivers mais recentes da Oracle devam apresentar compatibilidade retroativa, o teste do Sentinel foi executado com os drivers enviados junto com o banco de dados Oracle (por exemplo, os drivers 10.2.0.3 foram testados com o banco de dados 10.2.0.3).

Observação: O Sentinel não pode iniciar o banco de dados Oracle 10 devido a erros nos scripts `dbstart` e `dbshut` da Oracle. Modifique os scripts `dbstart` e `dbshut` depois de instalar o Sentinel. Para obter mais informações sobre como modificar esses scripts, consulte o Seção 3.8.7, “Modificando os scripts dbstart e dbshut da Oracle” na página 60.

Observação: Por motivos de desempenho, é altamente recomendável que, se estiver instalando em RAID ou se seu ambiente RAID permitir, você configure o sistema para que o Registro de Transação aponte para o disco de gravação mais rápido disponível, um disco físico separado em que os arquivos do banco de dados são armazenados.

  - É recomendável permitir que o instalador do Sentinel crie a instância do banco de dados Oracle para o Sentinel.
  - Se desejar, você poderá executar a criação da instância do banco de dados manualmente. Para garantir que a instância seja compatível com o Sentinel, consulte Seção B.2, “Criação manual de instância do Oracle (opcional)” na página 157. Se selecionar essa opção, você deverá executar o script fornecido pela Novell `createEsecDBA.sh` e usar o instalador do Sentinel para adicionar os objetos Banco de Dados à instância de banco de dados Oracle criada manualmente. Para obter mais informações, consulte a Seção 3.6, “Instalação Personalizada” na página 45.

Observação: Caso esteja usando uma instância de banco de dados Oracle existente ou criada manualmente, ela precisa estar vazia, exceto pela presença do Usuário do Banco de Dados do Sentinel.

- Obtenha credenciais de login para usuário do sistema operacional Oracle (padrão: oracle).
- Obtenha credenciais de login para SYSTEM e SYS.
- Verifique se as seguintes variáveis de ambiente estão definidas para o usuário do sistema operacional Oracle:
  - ORACLE_HOME (por exemplo, echo $ORACLE_HOME pode gerar /opt/oracle/product/10gR2/db)
  - ORACLE_BASE (por exemplo, echo $ORACLE_BASE gera /opt/oracle)
  - PATH (deve incluir $ORACLE_HOME/bin)
- Determine um número de porta de escuta Oracle apropriado (o padrão é 1521).
- No Linux/Solaris, crie diretórios para os seguintes locais de armazenamento:
  - Diretório de dados
  - Diretório de Índices
  - Diretório de Dados de Resumo
  - Diretório de Índices de Resumo

- Diretório Temp e Desfazer
- Diretório de Membro do Redo Log A
- Diretório de Membro do Redo Log B
- Diretório de Arquivos Reserva

Observação: Esses diretórios precisam permitir gravação pelo usuário do Oracle. Para tornar esses diretórios graváveis pelo usuário do Oracle, execute os comandos a seguir para cada diretório como usuário root:

chown –R oracle:dba <caminho_do_diretório>

chmod –R 770 <caminho_do_diretório>

- Depois de instalado no Oracle, o Banco de Dados do Sentinel conterá os seguintes usuários:
- **esecdba:** Proprietário do esquema de banco de dados. O privilégio DBA não é concedido ao Usuário do Banco de Dados do Sentinel devido a preocupações de segurança; portanto, para usar o Enterprise Manager, você deverá criar um usuário com privilégios DBA.
- **esecapp:** Usuário do aplicativo de banco de dados. Este é o usuário do aplicativo utilizado para a conexão com o banco de dados.
- **esecadm:** Usuário do banco de dados que é o Administrador do Sentinel. Não é a mesma conta do usuário do sistema operacional do Administrador do Sentinel.
- **esecrpt:** Usuário do relatório de banco de dados.
- **SYS:** Usuário SYS do banco de dados
- **SYSTEM:** Usuário SYSTEM do banco de dados

Pré-requisitos de instalação de banco de dados do Windows para o Sentinel

- O banco de dados do SQL Server deve estar instalado e em execução.
- O comando sc usado para iniciar o Serviço do Agente do SQL Server deve estar disponível no sistema operacional do seu banco de dados. (Se não estiver disponível, o Serviço do Agente do SQL Server deverá ser iniciado manualmente para que o particionamento e o arquivamento de dados funcionem corretamente. Além disso, esse serviço deverá ser programado para ser reiniciado após uma reinicialização do computador por outro utilitário.)
- Obtenha credenciais de login para o usuário do banco de dados do Administrador do Sistema
  - Se o banco de dados permitir a Autenticação do SQL, o usuário administrador do banco de dados padrão será sa.
  - Se o banco de dados estiver no Modo de Autenticação do Windows, você deverá executar o instalador quando efetuar login no Windows como usuário do banco de dados do Administrador do Sistema.
- Defina o serviço MSSQLSERVER para efetuar login usando a Conta Sistema Local.
- Determine o Nome da Instância do SQL Server, se aplicável.

Observação: Se você tiver especificado o nome da instância durante a instalação do SQL Server, use esse nome ao ser solicitado a fornecer o nome da instância do SQL Server quando instalar os componentes do Banco de Dados do Sentinel e/ou do DAS. Se não tiver especificado um nome para a instância durante a instalação do SQL Server, deixe o nome da instância em branco durante a instalação (ou seja, não adicione “\<nome_da_instância>” ao nome do host do banco de dados).

---

* Crie diretórios para os seguintes locais de armazenamento:
  * Diretório de dados
  * Diretório de Índices
  * Diretório de Dados de Resumo
  * Diretório de Índices de Resumo
  * Diretório de Registro
  * Diretório de Arquivos Reserva
* Determine o número da porta da instância do SQL Server (o padrão é 1433).

O sistema Sentinel usa diversas contas para instalação e operação do sistema. Essas contas estão situadas no banco de dados do Sentinel e podem usar a autenticação do SQL Server ou do Windows. Se você desejar usar a Autenticação do Windows para um ou mais usuários do Sentinel durante a instalação do Sentinel, o usuário do Domínio do Windows correspondente deverá existir antes da instalação do Banco de Dados do Sentinel.

O usuário do domínio deve ter privilégios de "Usuário Avançado" para iniciar os Serviços do Sentinel. Consulte a Seção 3.3.1, "Fornecendo privilégios de usuário avançado a "Usuários de Domínio"" na página 34 para obter mais informações.

Os usuários do Sentinel a seguir podem ser atribuídos a um usuário do domínio Windows:

* Administrador do Banco de Dados do Sentinel, utilizado como proprietário do esquema (chamado de esecdba por padrão quando a Autenticação do SQL é usada; pode ser qualquer conta de domínio quando a Autenticação do Windows é usada)
* Usuário do Aplicativo do Sentinel, utilizado por aplicativos do Sentinel para estabelecer conexão com o banco de dados (chamado de esecapp por padrão quando a Autenticação do SQL é usada; pode ser qualquer conta de domínio quando a Autenticação do Windows é usada)
* Administrador do Sentinel, utilizado como administrador do login no Sentinel Control Center (chamado de esecadm por padrão quando a Autenticação do SQL é usada; pode ser qualquer conta de domínio quando a Autenticação do Windows é usada)
* Usuário do Sentinel Reports, utilizado na criação de relatórios (chamado de esecrpt por padrão quando a Autenticação do SQL é usada; pode ser qualquer conta de domínio quando a Autenticação do Windows é usada)

Observação: Por padrão, o banco de dados contém o usuário do Administrador do Banco de Dados do Sentinel, o Usuário do Aplicativo do Sentinel e o usuário do Administrador do Sentinel

O Sentinel não suporta cluster da Microsoft ou Alta Disponibilidade para Windows.

Depois de instalado no SQL Server por meio da autenticação local, o Banco de Dados do Sentinel conterá os seguintes usuários:

* **esecdba:** Proprietário do esquema de banco de dados. O privilégio DBA não é concedido ao Usuário do Banco de Dados do Sentinel devido a preocupações de segurança; portanto, para usar o Enterprise Manager, você deverá criar um usuário com privilégios DBA.
* **esecapp:** Usuário do aplicativo de banco de dados. Este é o usuário do aplicativo utilizado para a conexão com o banco de dados.
* **esecadm:** Usuário do banco de dados que é o Administrador do Sentinel. Não é a mesma conta do usuário do sistema operacional do Administrador do Sentinel.

- **esecrpt:** Usuário do relatório de banco de dados.
- **sa:** Usuário do banco de dados do administrador do sistema.

3.3.3 Configurações do Modo de Autenticação no Microsoft SQL

No Windows, você precisa instalar o SQL Server com autenticação de modo misto para efetuar login no Sentinel Control Center usando a Autenticação do Windows ou do SQL Server. Se instalar o SQL Server com Autenticação do Windows, você só poderá efetuar login usando a Autenticação do Windows.

Para modificar suas configurações de modo de autenticação:

1. No Microsoft SQL Server Management Studio, clique o botão direito do mouse no servidor cujas configurações você deseja modificar.
2. Selecione Properties (Propriedades) e clique em Security (Segurança).
3. Nas opções Modo de Autenticação do SQL Server e do Windows (SQL Server and Windows Authentication Mode) ou Modo de Autenticação do Windows (Windows Authentication Mode), selecione a opção de autenticação desejada.

3.3.4 Pré-requisitos de instalação do Sentinel Server

Se não estiver instalando o Banco de Dados do Sentinel na mesma máquina que o Sentinel Server, você deverá instalar o Banco de Dados antes de instalar os outros componentes do Sentinel.

3.3.5 Pré-requisitos de instalação do Advisor

Para instalar o Advisor, você deverá adquirir os recursos opcionais de Inscrição de Dados do Advisor e de Detecção de Exploração do Sentinel. Em seguida, o eLogin da Novell receberá permissão para fazer downloads e atualizações de dados do Advisor.

Se você optar pelo Download Direto da Internet, a porta de saída 443 deverá ser aberta. Você deverá planejar a instalação do software Crystal Reports Server no sistema para executar relatórios.

Observação: Caso pretenda usar o Advisor somente para Detecção de Exploração, você não precisará instalar o software Crystal Reports Server. Para obter mais informações sobre os procedimentos de instalação, consulte o Capítulo 4, “Configuração do Advisor” na página 63.

3.4 Instalação do banco de dados

Um DBA testado deve fazer parte da instalação do Oracle ou do SQL Server. Além das recomendações do DBA, você também encontrará algumas recomendações da Novell para instalar o Oracle. Essas recomendações estão nas seguintes áreas:

- Definindo valores do Kernel
- No Solaris e no RHEL 4:
  - Criando uma conta de grupo e de usuário do Oracle

- Definindo as variáveis de ambiente
   - Verificando o layout do Solaris
- Instalação do Oracle
- Corrigindo o Oracle (se necessário)

3.4.1 Definindo valores do Kernel

Aviso: ISENÇÃO DE RESPONSABILIDADE: Os valores de Kernel sugeridos nesta seção são apenas valores mínimos. Você só deverá mudar essas configurações se as configurações do seu sistema forem inferiores aos valores mínimos recomendados e após consultar o administrador do sistema e a documentação do Oracle.

Para definir os valores do Kernel no Linux:

1. Efetue login como usuário root.
2. Faça uma cópia de backup de `/etc/sysctl.conf`.
3. Em um editor de texto, mude os parâmetros do kernel adicionando o seguinte texto ao final do arquivo "`/etc/sysctl.conf`":

   Observação: As configurações do kernel mostradas a seguir são as configurações mínimas recomendadas. Essas configurações poderão ser aumentadas se o hardware da máquina suportar.

   Para determinar a configuração atual de um determinado parâmetro de kernel, execute o comando:

   ```
   sysctl <kernel_parameter>
   ```

   Por exemplo, para verificar o valor atual do parâmetro de kernel "kernel.sem", execute o comando: `sysctl kernel.sem`

   Somente no SUSE LINUX 10 SP2:

   ```
   # Oracle requires MLOCK privilege for hugetlb memory.
   vm.disable_cap_mlock=1
   ```

   No REDHAT LINUX 4

   ```
   # Kernel settings for Oracle
   kernel.core_uses_pid = 1
   kernel.shmall = 2097152
   kernel.shmmax = 2147483648
   kernel.shmmni = 4096
   kernel.sem = 250 32000 100 128
   fs.file-max = 65536
   net.ipv4.ip_local_port_range = 1024 65000
   net.core.rmem_default = 262144
   net.core.rmem_max = 262144
   net.core.wmem_default = 262144
   net.core.wmem_max = 262144
   ```

4. Execute o seguinte comando para carregar as modificações no arquivo `/etc/sysctl.conf`:

```
sysctl -p
/sbin/sysctl –p (on RedHat Linux4)
```

5 Para definir os handles de arquivo e os limites de processo, adicione o texto a seguir ao final do arquivo "`/etc/security/limits.conf`". "nproc" é o limite máximo do número de processos, e "nofile" é o limite máximo do número de arquivos abertos. Trata-se de valores recomendados, mas que podem ser modificados se necessário. O texto a seguir supõe que seu ID de usuário do Oracle é "oracle".

```
# Settings added for Oracle
oracle          soft    nofile  65536
oracle          hard    nofile  65536
oracle          soft    nproc   16384
oracle          hard    nproc   16384
```

Para definir os valores do Kernel no Solaris 10:

No Oracle 10g:

noexec_user_stack=1	semsys:seminfo_semvmx=32767
semsys:seminfo_semmni=100	shmsys:shminfo_shmmax=4294967295
semsys:seminfo_semmns=1024	shmsys:shminfo_shmmni=100
semsys:seminfo_semmsl=256	

1 Por padrão, as instâncias do Oracle são executadas como o usuário oracle do grupo dba. O projeto `group.dba` será criado para ser o projeto padrão do usuário oracle. Execute o comando id para verificar o projeto padrão do usuário oracle.

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ exit
```

2 Para definir o tamanho máximo de memória compartilhada como 2 GB, execute o comando projmod

```
# projmod -sK "project.max-shm-memory=(privileged,2G,deny)"
group.dba
```

Como alternativa, você pode adicionar o controle de recurso project.max - `shm-memory=(privileged,2147483648,deny)` ao último campo de entradas do projeto oracle.

3 Depois que você concluir essas etapas, o arquivo /etc/project conterá o seguinte:

```
# cat /etc/project
```

4 Esta é a saída do comando:

```
system:0::::
user.root:1::::
noproject:2::::
default:3::::
group.staff:10::::
group.dba:100:Oracle default
project:::project.max-shmmemory=(privileged,2147483648,deny
```

5 Para verificar se o controle de recurso está ativo, execute os comandos id e prctl:

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ prctl -n project.max-shm-memory -i process $$
process: 5754: -bash
NAME PRIVILEGE VALUE FLAG ACTION RECIPIENT
project.max-shm-memory
privileged 2.00GB – deny
```

Observação: Para obter informações adicionais, consulte a documentação da Oracle para instalação do Solaris 10.

3.4.2 Criando conta de grupo e de usuário do Oracle (somente Solaris)

Para criar uma conta de grupo e de usuário e definir variáveis de ambiente:

1. Efetue login como usuário root.
2. Crie um grupo UNIX e uma conta de usuário UNIX para o proprietário do banco de dados Oracle.
   - Adicione um grupo dba (como root):
     `groupadd –g 400 dba`
   - Adicione o usuário oracle (como raiz) do shell csh:
     `useradd –g dba –d /export/home/oracle –m –s /bin/csh oracle`
   - Adicione o usuário oracle (como raiz) do shell bash:
     `useradd –g dba –d /export/home/oracle –m –s /bin/bash oracle`

3.4.3 Definindo variáveis de ambiente do Oracle (somente Solaris)

Para definir variáveis de ambiente:

1. Efetue login como usuário root.
2. Para definir as variáveis de ambiente necessárias para o Oracle no shell csh, sugerimos que você adicione as seguintes informações ao arquivo `local.cshrc`:

```
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
usr/ucb/etc.)
if ( $?prompt ) then
set history=32
endif
```

3. Para definir as variáveis de ambiente necessárias para o Oracle no shell bash, sugerimos que você adicione as seguintes informações ao arquivo `.profile` no diretório $ORACLE_HOME:

```
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
usr/ucb/etc.)
if ( $?prompt ) then
set history=32
endif
```

3.4.4 Instalar o Oracle

Para executar a instalação do Oracle, consulte o Apêndice B, "Instalação do Oracle" na página 153. Esta seção descreve as configurações de instalação recomendadas para operações do Sentinel. Ela também descreve os procedimentos para a criação da instância do Oracle. (A Novell recomenda que a instância seja criada com o instalador do Sentinel, mas fornece instruções para o caso de a política corporativa exigir que o DBA crie a instância manualmente.)

3.5 Instalação Simples

A opção Instalação Simples realiza uma instalação completa que inclui os Serviços do Sentinel, o Gerenciador de Coletor e os Aplicativos do Sentinel com o banco de dados na mesma máquina. Esse tipo de instalação destina-se apenas a demonstrações e treinamentos e, portanto, não deve ser usado em ambientes de produção.

Depois de executar a instalação do banco de dados e atender aos pré-requisitos mencionados na seção anterior, você poderá continuar com a instalação do Sentinel. Se a Instalação Simples for escolhida, algumas pressuposições serão feitas e diversas configurações padrão serão usadas:

- No Windows, a Autenticação do SQL será permitida no banco de dados do SQL Server.
- A mesma senha será usada para o Administrador do Banco de Dados do Sentinel, o Administrador do Sentinel, o Usuário do Aplicativo do Sentinel e o Usuário do Sentinel Reports.
- O Advisor será configurado para usar Download Direto da Internet.
- O Advisor será configurado para fazer o download de novas informações a cada 12 horas.
- O recursos de notificações por e-mail do Advisor estará habilitado.
- O tamanho do banco de dados será de 10GB.

Para instalar o Sentinel:

1. Efetue login como usuário root no Solaris/Linux ou usuário administrador no Windows.
2. Insira e monte o CD de instalação do Sentinel.
3. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e
   - No Windows, execute `setup.bat`
   - No Solaris/Linux:

     Para o modo de interface gráfica:

     `./setup.sh`

     Para o modo baseado em texto ("console serial"):

```
./setup.sh -console
```

Observação: Você não poderá executar o instalador no UNIX se o caminho do diretório contiver espaços.

4 Clique na seta para baixo e selecione uma das seguintes opções de idioma:

Inglês	Italiano
Francês	Português (Brasil)
Alemão	Espanhol
Chinês Simplificado	Japonês
Chinês Tradicional	

5 Depois de ler a tela de boas-vindas, clique em Avançar.

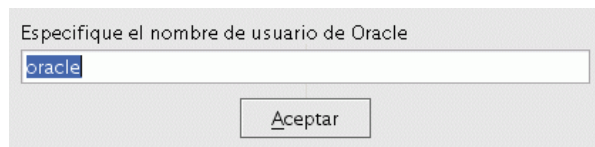
6 Leia e aceite o Contrato de Licença de Usuário Final. Clique em Avançar.

7 Aceite o diretório de instalação padrão ou clique em Procurar para especificar o local da instalação. Clique em Avançar.

Observação: Você não pode realizar a instalação em um diretório com caracteres especiais ou caracteres que não sejam ASCII. Por exemplo, quando você instalar o Sentinel 6.1 no Windows x86-64, o caminho padrão será C:\Arquivos de Programas (x86). Se desejar continuar com a instalação, você deverá mudar o caminho padrão para evitar os caracteres especiais.

8 Selecione Simples. Clique em Avançar.

9 Nessa janela, forneça as informações de configuração e clique em Avançar.

- Número de Série
- Chave de Licença
- SMTP Server
  - O Sentinel envia e-mails por meio desse servidor.
- E-mail
  - Os e-mails enviados pelo Sentinel exibem esse endereço como endereço de e-mail do remetente.
- Senha do Sistema Global
- A senha que você digitar aqui será válida para todos os usuários padrão. Isso inclui o usuário do Administrador do Sentinel e os usuários do banco de dados. Para obter mais informações sobre a lista de usuários de banco de dados padrão criados com a instalação, consulte a Seção 3.8.2, “Banco de Dados do Sentinel” na página 58.
- Nome de Usuário e Senha do Advisor (opcional)
  - Para instalar o Advisor, especifique um eLogin e uma senha da Novell associados à licença do Advisor. Forneça sua senha do Advisor novamente na janela de confirmação de senha.

Observação: Nomes de usuário e senhas fornecidos pelo Advisor antes do Sentinel 6.0 SP2 não são mais válidos. Use o eLogin da Novell e a senha associada à licença do Advisor. Em algumas organizações, há mais de um indivíduo com eLogin da Novell. O eLogin usado para downloads do Advisor deve ser associado à aquisição do Advisor.

---

10 Em Configuração do Banco de Dados:

- Selecione a plataforma de Banco de Dados de destino.

No Solaris/Linux, você será solicitado a especificar o nome de usuário do Oracle. Forneça o nome de usuário e clique em OK.

Figura 3-4 *Campo para especificação do nome de usuário do Oracle*

Fornecer Nome do Banco de Dados

- No Linux/Solaris, especifique o arquivo de driver JDBC do Oracle.
- No Windows, forneça credenciais de usuário do banco de dados e nome de instância do SQL Server.

Clique em Avançar.

Observação: No Linux/Solaris, o instalador faz backup de todos os arquivos `tnsnames.ora` e `listener.ora` no diretório $ORACLE_HOME/network/admin. Ele sobregravará o arquivo `listener.ora` com informações de conexão de banco de dados do Sentinel e anexará as informações de conexão do banco de dados do Sentinel ao arquivo `tnsnames.ora`. Se houver outros bancos de dados no mesmo servidor do banco de dados do Sentinel, o administrador deverá fundir manualmente as informações dos arquivos `listener.ora` de backup com o novo arquivo e reiniciar a escuta do Oracle para que outros aplicativos possam continuar se conectando ao banco de dados.

Figura 3-5 *Resumo dos parâmetros de banco de dados*

Um banco de dados MSSQL será criado com os seguintes parâmetros:
Será criado um novo banco de dados com o nome: **ESEC617**
Este banco de dados terá um tamanho inicial de **1000 MB**.
Esse banco de dados terá o tamanho máximo de **20000 MB**.

As localizações dos armazenamentos dos arquivos de dados serão as seguintes:
Arquivos de Dados: **D:\esecdata**
Arquivos de Índice: **D:\esecdata**
Arquivos de Dados de Resumo: **D:\esecdata**
Arquivos de Índice de Resumo: **D:\esecdata**
Arquivos de Registro: **D:\esecdata**

O proprietário do esquema será: **esecdba**
O usuário do Aplicativo Sentinel será: **$v(Esec_APP_LOGIN)**
O Administrador do Sentinel será: **esecadm**
O Usuário do Sentinel Report será: **esecrpt**

11 O resumo dos parâmetros de banco de dados selecionados é exibido. Clique em Avançar.

12 O resumo da instalação é exibido. Clique em Instalar.

13. Após a instalação, clique em Concluir.
14. Reinicialize o sistema. (Os serviços programados, como o download do Advisor, só funcionarão após a reinicialização.)

3.6 Instalação Personalizada

A opção Instalação Personalizada permite a realização de uma instalação totalmente distribuída, com mais controle sobre memória e outras configurações de instalação. A opção Instalação Personalizada pode ser usada para instalar um ou mais componentes do Sentinel, incluindo:

- Componentes do Banco de Dados do Sentinel
- Serviços do Sentinel
  - Servidor de Comunicação
  - Advisor
  - Mecanismo de Correlação
  - DAS (Serviço de Acesso a Dados)
  - Serviço do Coletor do Sentinel (Gerenciador de Coletor)
- Aplicativos
  - Sentinel Control Center
  - Gerenciador de Dados do Sentinel
  - Designer de Soluções do Sentinel
- Integração de Terceiros
  - HP OpenView Service Desk

Depois de atender aos pré-requisitos mencionados na seção anterior, você poderá continuar com a instalação do Sentinel.

Os Componentes do Banco de Dados do Sentinel devem ser sempre instalados primeiro. Os outros componentes poderão ser instalados simultaneamente se a arquitetura do sistema incluir vários componentes na máquina do banco de dados. O procedimento descrito a seguir mostra as etapas necessárias para instalar todos os componentes na mesma máquina; a instalação distribuída incluirá um subconjunto das etapas abaixo.

Para instalar o Sentinel:

1. Efetue login como usuário root no Solaris/Linux ou usuário administrador no Windows.

   Observação: A instalação do componente Banco de Dados do Sentinel no Windows quando a instância do MS SQL Server de destino estiver no Modo de Autenticação do Windows exigirá que você efetue login no Windows como usuário do banco de dados do Administrador do Sistema.

2. Insira e monte o CD de instalação do Sentinel.
3. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e
   - No Windows, execute `setup.bat`
   - No Solaris/Linux:

     Para o modo de interface gráfica:

```
./setup.sh
```

Para modo textual (“sem cabeçalho”):

```
./setup.sh -console
```

Observação: Você não poderá executar o instalador no UNIX se o caminho do diretório contiver espaços.

4 Clique na seta para baixo e selecione uma das seguintes opções de idioma:

Inglês	Italiano
Francês	Português (Brasil)
Alemão	Espanhol
Chinês Simplificado	Japonês
Chinês Tradicional	

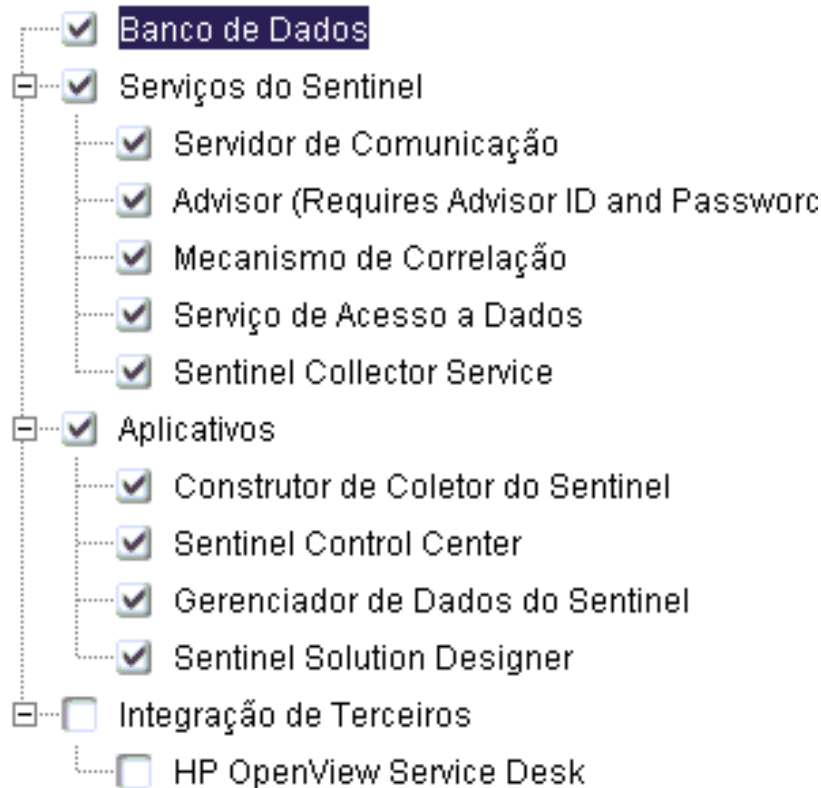
5 Depois de ler a tela de boas-vindas, clique em Avançar.

6 Leia e aceite o Contrato de Licença de Usuário Final. Clique em Avançar.

7 Aceite o diretório de instalação padrão ou clique em Procurar para especificar o local da instalação. Clique em Avançar.

Observação: Você não pode realizar a instalação em um diretório com caracteres especiais ou caracteres que não sejam ASCII.

8 Selecione Personalizada. Clique em Avançar.

9 Selecione os componentes do Sentinel a serem instalados.

As seguintes opções estão disponíveis:

Componente	Descrição
Banco de Dados	Instala os objetos Banco de Dados do Sentinel (tabelas, telas, procedimentos armazenados, etc.) em uma instância de banco de dados. Opcionalmente, cria a instância de banco de dados primeiro.
Servidor de Comunicação	Instala o barramento de mensagem (iSCALE) e o Proxy DAS.
Mecanismo de Correlação	Instala o mecanismo de correlação.
Advisor	Instala os componentes relacionados ao serviço de inscrição de dados do Advisor. Requer uma licença do Advisor e deve residir na mesma máquina que o DAS.
DAS (Serviço de Acesso a Dados)	Instala componentes que se comunicam com o banco de dados do Sentinel. Requer uma chave de licença e um número de série do Sentinel. (Necessário para a instalação do Advisor.)
Serviço do Coletor do Sentinel	Instala o Gerenciador de Coletor, que administra conexões com fontes de eventos, análises de dados, mapeamentos, etc.
Sentinel Control Center	Instala o console principal para analistas de segurança e conformidade.
SDM (Gerenciador de Dados do Sentinel)	Instala o SDM, que é usado para atividades manuais de gerenciamento de banco de dados.

Componente	Descrição
Designer de Soluções	Instala o Designer de Soluções
HP OpenView Service Desk	Instala a integração com o HP OpenView Service Desk. Requer licença.

Observação: Há um tempo de atraso na interface quando você seleciona ou anula a seleção de um componente.

Observação: Se nenhum dos recursos filhos de Serviços do Sentinel for selecionado, anule a seleção do recurso Serviços do Sentinel também. Ele ficará esmaecido (indisponível) com uma marca de seleção branca se ainda estiver selecionado, mas todos os recursos filhos serão desmarcados.

Observação: Como parte da instalação do componente Banco de Dados de Sentinel, o instalador colocará arquivos na pasta %ESEC_HOME%\ unist\db.

Observação: Se você usar o modo "console", a página de seleção de componentes não exibirá todos os componentes juntos. Siga as instruções na tela para ver e editar os componentes filhos selecionados. Nem todos os componentes filhos são selecionados por padrão. Para obter informações, consulte a Seção 3.6.1, "Instalação de console no Linux/Solaris" na página 56.

10 Se optar por instalar o DAS, você será solicitado a fornecer:
   - Número de Série
   - Chave de Licença

11 No Linux/Solaris, especifique o nome de usuário do Administrador do Sentinel do sistema operacional e a localização do diretório pessoal. Esse é o nome de usuário que terá a propriedade do produto Sentinel instalado. Se o usuário não existir ainda, um usuário será criado com um diretório pessoal no diretório especificado.
   - Nome de usuário do Administrador do Sentinel do sistema operacional – O padrão é esecadm
   - Diretório pessoal do usuário do Administrador do Sentinel do sistema operacional – O padrão é "/export/home". Se o nome de usuário for esecadm, o diretório pessoal do usuário será /export/home/esecadm.

Observação: Para atender às configurações de segurança rígidas exigidas pela Certificação de Critérios Comuns.

Observação: O usuário esecadm será criado sem a definição de uma senha. Para efetuar login como esse usuário, você precisará primeiro definir a senha.

12 Se você optar por instalar o Sentinel Control Center, o instalador solicitará que o espaço em memória máximo seja alocado para o Sentinel Control Center. Especifique o tamanho de heap JVM máximo (MB) que você deseja que seja usado somente pelo Sentinel Control Center.
   - **Tamanho de heap JVM (MB):** O padrão é 256 MB. O valor máximo pode ser 1024 MB.

Configuración del Centro de control de Sentinel

Especifique el tamaño de pila JVM para el Centro de control de Sentinel. El instalador ha detectado 1038 MB de memoria físico. El rango permitido es de 64 a 1.024.

Tamaño de la pila JVM (MB)

256

13 Se optar por instalar o Gerenciador de Coletor e não instalar o DAS (Serviço de Acesso a Dados), você poderá estabelecer comunicação entre os Gerenciadores de Coletor do Sentinel e o Sentinel Server de duas maneiras. Você poderá selecionar a comunicação do tipo Barramento de Mensagem Direta ou a comunicação do tipo Proxy. Para obter mais informações sobre essas opções, consulte o Capítulo 7, "Camada de comunicação (iSCALE)" na página 91.

Observação: Se selecionar a comunicação do tipo Proxy, imediatamente após a conclusão da instalação você será solicitado a fornecer informações necessárias para registrar o Gerenciador de Coletor como cliente confiável. Isso requer que o Servidor de Comunicação esteja em execução.

Se o Servidor de Comunicação não estiver disponível, selecione a comunicação do tipo Barramento de Mensagem Direta e mais tarde configure manualmente a comunicação do tipo Proxy executando a Etapa 26 na página 55 (Configurando a comunicação do tipo Proxy).

Seleccione cómo debe conectarse el Gestor de recopiladores al bus de mensaje:

- (•) Conectarse directamente al bus de mensaje.
- ( ) Conectarse al bus de mensaje utilizando el alterno (proxy).

14 Você é solicitado a fornecer o nome do servidor de host ou da porta do Servidor de Comunicação. Forneça as informações solicitadas e clique em Avançar.

- **Porta de barramento de mensagem:** a porta de escuta do servidor de comunicação. Os componentes que se conectarem diretamente ao servidor de comunicação usarão essa porta.
- **Porta proxy do Sentinel Control Center:** a porta em que o servidor proxy SSL (Proxy DAS) escuta para aceitar conexões autenticadas baseadas no nome de usuário e na senha. Como solicita um nome de usuário e uma senha, o Sentinel Control Center usa essa porta para se conectar ao Sentinel Server.
- **Porta Proxy de Autenticação do Certificado do Gerenciador de Coletor:** a porta em que o servidor proxy SSL (Proxy DAS) escuta para aceitar conexões autenticadas baseadas em certificação. Como não pode solicitar um nome de usuário e uma senha, o Gerenciador de Coletor usará essa porta para se conectar ao Sentinel Server se estiver configurado para se conectar usando o proxy.

Observação: Os números de porta devem ser idênticos em todas as máquinas do sistema Sentinel para permitir a comunicação. Anote essas portas para instalações futuras em outras máquinas.

15 Se estiver instalando um componente que fará uma conexão direta com o barramento de mensagem ou se estiver instalando o Servidor de Comunicação, você será solicitado a informar como obter a chave criptográfica compartilhada de barramento de mensagem:

- Gerar uma chave criptográfica aleatória.
- Importar uma chave criptográfica do arquivo keystore. Você será solicitado a navegar até um arquivo .keystore existente.

Selecione como obter a chave de criptografia de barramento de mensagem:

(•) Gerar uma chave de criptografia de barramento de mensagem aleatória.

Gera uma chave de criptografia aleatória para comunicação de barramento de mensagem e a armazena no arquivo keystore. Normalmente, esta opção é utilizada apenas ao instalar o Servidor de Comunicação.

( ) Importar uma chave de criptografia de barramento de mensagem do arquivo k...

Importa a chave de criptografia de barramento de mensagem do arquivo keystore existente. Use esta opção ao instalar componentes que se conectam diretamente ao barramento de mensagem e para os quais já tenha sido criada uma chave em algum lugar. A chave importada deve corresponder à chave utilizada pelo Servidor de Comunicação.

Observação: Todos os componentes que se conectam diretamente ao barramento de mensagem devem compartilhar a mesma chave criptográfica. A Novell recomenda gerar uma chave criptográfica aleatória ao instalar o Servidor de Comunicação e importar essa chave ao instalar os componentes em outras máquinas. Os componentes que se conectam por meio do proxy não precisam da chave criptográfica de barramento de mensagem.

O arquivo .keystore será colocado em $ESEC_HOME/config no Linux/Solaris ou em %ESEC_HOME%\config no Windows.

16 Selecione a plataforma do Servidor do Banco de Dados de destino. Clique em Avançar. Se você optar por instalar o DAS, e os Componentes do Banco de Dados do Sentinel já estiverem instalados, você será solicitado a fornecer as informações a seguir do Banco de Dados do Sentinel. Essas informações serão usadas para configurar o DAS para que aponte para o Banco de Dados do Sentinel.

- **Endereço IP ou nome de host do banco de dados:** O nome ou o IP do Banco de Dados do Sentinel existente em que eventos e informações de configuração serão armazenados.
- **Nome do banco de dados:** O nome da instância do Banco de Dados do Sentinel a ser configurada para se conectar ao componente DAS (o padrão é ESEC).
- **Porta do banco de dados:** (padrão - Microsoft SQL Server:1433 e Oracle:1521)
- **Usuário de Banco de Dados do Aplicativo Sentinel:** Especifique o login do Usuário do Aplicativo do Sentinel (o padrão é esecapp) e a senha fornecida a esse usuário durante a instalação do Banco de Dados do Sentinel.

Clique em Avançar.

17 Se optar por instalar o banco de dados, configure-o para instalação:

No Windows:

- Selecione o Microsoft SQL Server 2005 ou o Microsoft SQL Server 2008 como plataforma de servidor de banco de dados de destino.
  - **Criar um novo banco de dados com objetos Banco de Dados:** Cria um novo banco de dados Microsoft SQL e também preenche o novo banco de dados com objetos Banco de Dados.
  - **Adicionar objetos Banco de Dados a um banco de dados vazio existente:** Só adiciona objetos Banco de Dados a um banco de dados Microsoft SQL Server 2005 existente. O banco de dados existente precisa estar vazio.
  - Especifique o diretório do registro de Instalação do Banco de Dados.

  Clique em Avançar.
- Se estiver criando um banco de dados novo, especifique os diretórios existentes a serem usados como armazenamento para:
  - Diretório de dados
  - Diretório de Índices
  - Diretório de Dados de Resumo
  - Diretório de Índices de Resumo
  - Diretório de Registro

  Clique em Avançar.
- Se estiver criando um banco de dados novo, selecione a opção de suporte de conjunto de caracteres do banco de dados; banco de dados Unicode ou Apenas ASCII. Se o instalador estiver sendo executado em um idioma asiático, a opção de banco de dados Unicode será definida por padrão. Se o instalador estiver sendo executado em um idioma não-asiático, o sistema solicitará que você selecione Apenas ASCII ou Unicode, escolha um formato de banco de dados e clique em OK.

  Observação: A instalação de banco de dados Unicode requer mais espaço em disco rígido do que a instalação Apenas ASCII.

- Se estiver criando um banco de dados novo, selecione uma opção de tamanho de banco de dados. Clique em Avançar.
- Se estiver criando um banco de dados novo e o tamanho de banco de dados personalizado for selecionado, especifique as configurações do tamanho de banco de dados personalizado:
  - **Tamanho Máximo de Banco de Dados:** O volume máximo de espaço em disco a ser ocupado pelo banco de dados. À medida que acumular dados, o banco de dados aumentará automaticamente até atingir o tamanho definido. Independentemente do valor especificado, o tamanho inicial do banco de dados será de 1000 MB.
  - **Tamanho do Arquivo de Registro:** O tamanho do arquivo de registro de transação.
  - **Tamanho Máximo de Arquivo de Banco de Dados:** O tamanho de nenhum arquivo de banco de dados ultrapassará esse valor.

  Clique em Avançar.

No Linux/Solaris:

- Determine a versão do servidor de banco de dados Oracle e selecione o seguinte:
  - **Criar um novo banco de dados com objetos Banco de Dados:** Cria uma nova instância de banco de dados Oracle e também preenche o novo banco de dados com objetos Banco de Dados
  - **Adicionar objetos Banco de Dados a um banco de dados vazio existente:** Só adiciona objetos Banco de Dados a uma instância existente de banco de dados Oracle. O banco de dados existente precisa estar vazio, exceto pela presença do usuário esecdba.
  - Especifique o diretório do registro de Instalação do Banco de Dados.

  Clique em Avançar.
- Especifique o Nome de Usuário do Oracle ou Aceite o nome de usuário padrão. Clique em OK.
- Se você optar por criar um novo banco de dados, especifique o seguinte:
  - **O caminho para o arquivo do driver JDBC da Oracle:** Especifique o caminho completo para o arquivo jar, normalmente `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (no entanto, não use variáveis de ambiente nesse campo).
  - **Nome do host:** O nome de host da máquina local em que o banco de dados Oracle está instalado. O instalador só suporta a criação de uma nova instância do banco de dados no host local.
  - **Nome do banco de dados:** O nome da instância do banco de dados a ser criada.
- Se optar por adicionar objetos Banco de Dados a um banco de dados Oracle vazio existente, você será solicitado a fornecer as informações a seguir.
  - **O caminho para o arquivo do driver JDBC da Oracle:** Especifique o caminho completo para o arquivo jar, normalmente `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (no entanto, não use variáveis de ambiente nesse campo).
  - **Endereço IP ou nome de host do banco de dados:** O nome de host ou o endereço IP da máquina em que o banco de dados Oracle está instalado. Pode ser o nome de host local ou um nome de host remoto.
  - **Nome do banco de dados:** O nome da instância vazia existente do banco de dados Oracle (o padrão é ESEC). Esse nome de banco de dados precisa ser exibido como um nome de serviço no arquivo `tnsnames.ora` (no diretório $ORACLE_HOME/network/admin/) da máquina em que o instalador está sendo executado.
  - **Porta do banco de dados:** O padrão é 1521
  - **Senha:** Para o Usuário Administrador do Banco de Dados do Sentinel (DBA), especifique a senha do usuário "esecdba". O campo Nome de Usuário desse prompt não pode ser editado.

Observação: Se o nome do banco de dados não estiver no arquivo `tnsnames.ora`, o instalador não exibirá um erro nesse momento da instalação (porque ele verifica a conexão usando uma conexão JDBC direta), mas ocorrerá falha na instalação do Banco de Dados quando o instalador tentar se conectar ao banco de dados por meio do sqlplus. Se a instalação do Banco de Dados falhar nesse ponto, modifique o Nome do Serviço do banco de dados no arquivo `tnsnames.ora` dessa máquina, sem sair do instalador, volte uma tela no instalador e, em seguida, avance novamente. A instalação do Banco de Dados será repetida com os novos valores no arquivo `tnsnames.ora`.

Observação: O instalador fará backup de todos os arquivos `tnsnames.ora` e `listener.ora` no diretório $ORACLE_HOME/network/admin. Ele sobregravará o arquivo `listener.ora` com informações de conexão de banco de dados do Sentinel e anexará as informações de conexão do banco de dados do Sentinel ao arquivo `tnsnames.ora`. Se houver outros bancos de dados no mesmo servidor do banco de dados do Sentinel, o administrador deverá fundir manualmente as informações dos arquivos `listener.ora` de backup com o novo arquivo e reiniciar a escuta do Oracle para que outros aplicativos possam continuar a se conectar ao banco de dados.

- Se estiver criando uma nova instância de banco de dados, especifique a alocação de memória (RAM) e a porta de escuta do Oracle ou aceite os valores padrão.
- Se estiver criando uma nova instância de banco de dados, especifique as senhas a serem definidas para os usuários SYS e SYSTEM padrão do banco de dados. Clique em Avançar.
- Se estiver criando uma nova instância de banco de dados, selecione uma opção de tamanho de banco de dados. Clique em Avançar.
- Se estiver criando uma nova instância de banco de dados e o tamanho de banco de dados personalizado for selecionado, especifique as configurações do tamanho de banco de dados personalizado:
    - **Tamanho Máximo de Banco de Dados:** O volume máximo de espaço em disco a ser ocupado pelo banco de dados. À medida que acumular dados, o banco de dados aumentará automaticamente até atingir o tamanho definido. Independentemente do valor especificado, o tamanho inicial do banco de dados será de 5000 MB.
    - **Tamanho do Arquivo de Registro:** O tamanho de cada arquivo redo log.
    - **Tamanho Máximo de Arquivo de Banco de Dados:** O tamanho de nenhum arquivo de banco de dados ultrapassará esse valor.
- Se estiver criando uma nova instância de banco de dados, especifique os diretórios existentes a serem usados como armazenamento de banco de dados:
    - Diretório de dados
    - Diretório de Índices
    - Diretório de Dados de Resumo
    - Diretório de Índices de Resumo
    - Diretório Temp e Desfazer
    - Diretório de Membro do Redo Log A
    - Diretório de Membro do Redo Log B

  Clique em Avançar.

Observação: Para fins de recuperação e desempenho, a Novell recomenda que esses locais estejam em dispositivos de E/S diferentes.

Por motivos de desempenho, o Redo Log deve apontar para o disco de gravação mais rápido disponível.

O instalador não criará esses diretórios, portanto, eles devem ser criados externamente, antes do fim desta etapa. Além disso, é preciso que esses diretórios possam ser gravados pelo usuário oracle. Para obter mais informações, consulte a Seção 3.3.2, “Pré-requisitos de instalação do Banco de Dados do Sentinel” na página 34.

18 Se optar por instalar o componente de banco de dados, configure partições de banco de dados.

- Selecione Habilitar partições automáticas de banco de dados para permitir que o Gerenciador de Dados do Sentinel administre o particionamento e o arquivamento de bancos de dados.
- Para partições de dados, especifique um diretório existente para arquivamento.
- Especifique o horário de início para a adição de partições e o arquivamento de dados. Essas operações não podem se sobrepor, pois usam recursos compartilhados.

Clique em Avançar.

19 Se optar por instalar o componente de banco de dados, forneça informações de autenticação para:

- Usuário Administrador do Banco de Dados do Sentinel
- Usuário de Banco de Dados do Aplicativo Sentinel
- Usuário Administrador do Sentinel
- Usuário do Sentinel Reports (somente no Windows)

Observação: Se o componente DAS também estiver sendo instalado, a senha do Usuário do Banco de Dados do Aplicativo do Sentinel será exigida mesmo que a Autenticação do Windows seja selecionada. Isso é necessário para instalar o Serviço do Sentinel e “Efetuar login como” Usuário do Banco de Dados do Aplicativo do Sentinel. Não será necessário especificar senha para nenhum outro usuário se a Autenticação do Windows estiver sendo usada.

Clique em Avançar.

20 Se você optar por instalar o componente de banco de dados, será exibido um resumo dos parâmetros de Banco de Dados especificados. Clique em Avançar.

21 Se optar por instalar um dos componentes do Sentinel Server, você será solicitado a especificar o volume de memória (RAM) a ser alocado para esses componentes. O instalador será dividido em overhead de sistema operacional e de banco de dados quando for determinado quais opções de alocação devem ser exibidas. Você pode especificar a alocação de memória de duas maneiras:

- **Configuração Automática de Memória:** Selecione o volume total de memória a ser alocado para o Sentinel Server. O instalador determinará automaticamente a distribuição ideal de memória entre os componentes, levando em consideração o overhead estimado do sistema operacional e do banco de dados.

  Importante: Você pode modificar o valor -Xmx no arquivo `configuration.xml` para mudar a RAM alocada para os processos do Sentinel Server. O arquivo `configuration.xml` é colocado em `$ESEC_HOME/config` no Linux/Solaris ou em `%ESEC_HOME%\config` no Windows.

- **Configuração Personalizada de Memória:** Clique no botão Configurar… para ajustar as alocações de memória. Essa opção só estará disponível se houver memória suficiente na máquina.

22 Se você optar por instalar o Advisor, será exibido o seguinte prompt solicitando o tipo de atualização:

- **Download Direto da Internet:** Nessa configuração, as atualizações da Novell são transferidas por download automaticamente através da Internet em horários regulares (a cada 6 ou 12 horas). Use essa opção se a máquina tiver acesso direto à Internet.
- **Independente:** Nessa configuração, a atualização do Advisor exige o download manual de arquivos da Novell. Use essa opção se a máquina não tiver acesso direto à Internet.

23 Se optar por instalar o Advisor e tiver selecionado Download Direto da Internet, forneça um eLogin da Novell e a senha associada à licença do Advisor e informe com que freqüência os dados do Advisor devem ser atualizados (a cada 6 ou 12 horas). Clique em Avançar.

24 Se você optar por instalar o Advisor, forneça o seguinte:

- Endereço do remetente, que será exibido em notificações por e-mail relacionadas ao Advisor
- Endereço do destinatário, para o envio de notificações por e-mail relacionadas ao Advisor

Observação: Após a instalação, você poderá mudar os endereços de e-mail do Advisor editando a seção AdvisorService do arquivo `advisor_client.xml` no diretório $ESEC_HOME/config. Para obter mais informações, consulte a "Guia Advisor" no *Guia do Usuário do Sentinel*.

- Selecione Sim ou Não para o recebimento de e-mails sobre atualizações bem-sucedidas do Advisor.

Observação: Notificações de erro serão sempre enviadas, independentemente da opção selecionada.

Observação: Se optar por instalar o HP Service Desk, você será solicitado a fornecer mais informações.

25 Clique em Avançar. Será exibida a tela de resumo com os recursos selecionados para instalação. Clique em Instalar.

26 Se optar por instalar o Gerenciador de Coletor e ele for configurado para usar comunicação do tipo Proxy, você será solicitado a fornecer o nome de usuário e a senha de um usuário do Sentinel que tenha permissão para registrar um cliente confiável (por exemplo, esecadm). Para concluir esta etapa, execute o Servidor de Comunicação e especifique um nome de usuário e uma senha válidos. Para registrar um cliente confiável, é necessário aceitar o certificado SSL do Servidor de Comunicação e fazer upload do certificado SSL do Gerenciador de Coletor para o Servidor de Comunicação. Quando a conexão com o Servidor de Comunicação é iniciada, você é solicitado a aceitar a certificação do servidor. Depois de analisar os atributos da certificação, selecione "Aceitar Permanentemente". Em seguida, o instalador fará automaticamente o upload do certificado do Gerenciador de Coletor para o Servidor de Comunicação.

27 Após a instalação, você será solicitado a reinicializar o sistema ou a efetuar outro login e a iniciar os Serviços do Sentinel manualmente. Clique em Concluir para reinicializar o sistema. (Os serviços programados, como o download do Advisor, só funcionarão após a reinicialização.)

Observação: O instalador do Sentinel desliga o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos; caso contrário, o banco de dados não aceitará mais eventos.

3.6.1 Instalação de console no Linux/Solaris

Se você usar o modo "console", a página de seleção de componentes do instalador não exibirá todos os componentes juntos. Siga as instruções na tela para ver e editar os componentes filhos selecionados.

Veja a seguir um exemplo de como navegar na página de seleção de componentes do modo console:

```
Sentinel 6.1 - InstallShield Wizard
Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
   To select/deselect a feature or to view its children, type its
number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 1

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
   To select/deselect a feature or to view its children, type its
number:
     1.  [x] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 2
    1. Deselect 'Sentinel Services'
    2. View 'Sentinel Services' subfeatures
    Enter command [1] 2

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services

      To select/deselect a feature or to view its children, type its
number:
        1.  [ ] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        5.  [x] Sentinel Collector Service
```

```
        Other options:
         -1. View this feature's parent
          0. Continue installing
        Enter command [0] 1

Select the features for "Sentinel 6.1" you would like to install:
    Sentinel 6.1
     - Sentinel Services
        To select/deselect a feature or to view its children, type its
number:
          1.  [x] Communication Server
          2.  [ ] Advisor (Requires Advisor ID and Password)
          3.  [x] Correlation Engine
          4.  [x] Data Access Server
          5.  [x] Sentinel Collector Service
        Other options:
         -1. View this feature's parent
          0. Continue installing
        Enter command [0] 2

Select the features for "Sentinel 6.1" you would like to install:
    Sentinel 6.1
     - Sentinel Services
        To select/deselect a feature or to view its children, type its
number:
          1.  [x] Communication Server
          2.  [x] Advisor (Requires Advisor ID and Password)
          3.  [x] Correlation Engine
          4.  [x] Data Access Server
          5.  [x] Sentinel Collector Service
         Other options:
          -1. View this feature's parent
          0. Continue installing
```

3.7 Instalando o Sentinel como usuário de domínio

Para instalar o Sentinel como usuário de domínio:

1. Mapeie um usuário de domínio para um dos usuários do Sentinel (esecdba, esecadm, esecrpt).
2. Execute as ações mencionadas na Seção 3.3.1, “Fornecendo privilégios de usuário avançado a “Usuários de Domínio”” na página 34 para fornecer privilégios de usuário avançado.
3. Instale o Sentinel 6.0 como usuário administrador. Consulte a Seção 3.6, “Instalação Personalizada” na página 45 para instalar o Sentinel.
4. Quando o instalador solicitar as credenciais do usuário esecdba, esecadm e esecrpt, especifique o usuário de domínio criado no formato “domínio\usuário de domínio”, forneça a senha e continue com a instalação.
5.

3.8 Configuração de pós-instalação

3.8.1 Configurando o integrador SMTP para enviar notificações do Sentinel

No Sentinel 6.1, a ação `Enviar E-mail` do JavaScript funciona com um integrador do SMTP para enviar mensagens de vários contextos da interface do Sentinel para destinatários de e-mail. Os destinatários e o conteúdo da mensagem de e-mail são configurados nos parâmetros da ação.

Uma única instância de ação do plug-in `Enviar E-mail` é criada automaticamente em cada instalação do Sentinel. Essa ação é usada internamente pelo Sentinel para enviar e-mails nas seguintes situações:

- Quando uma regra de correlação implantada com uma ação Enviar E-mail é acionada. A ação Enviar E-mail mencionada aqui é a ação indicada pelo ícone de engrenagem, válida somente para correlação (e não a ação `Enviar E-mail` do JavaScript, indicada pelo ícone do JS JavaScript).
- O workflow inclui uma Atividade ou uma Etapa de E-mail configurada para enviar e-mails.
- O usuário abre um incidente e especifica que deseja executar uma Atividade configurada para enviar e-mails.
- O usuário clica o botão direito do mouse em um evento e seleciona E-mail.
- O usuário abre um incidente e seleciona Incidente de E-mail.
- O download do Advisor envia uma notificação.

Não é necessário configurar a ação `Enviar E-mail`, mas o integrador do SMTP deve ser configurado com informações de conexão válidas.

3.8.2 Banco de Dados do Sentinel

A não ser que o DBA deseje gerenciar o arquivamento de bancos de dados usando seus próprios procedimentos, o gerenciamento de partição automático do banco de dados do Sentinel (arquivamento, descarte e adição de partições) deverá ser habilitado durante a instalação para que o tamanho dos dados de evento seja controlado. O gerenciamento de partição automática também pode ser configurado após a instalação com o SDM (Gerenciador de Dados do Sentinel).

Por padrão, o Gerenciador de Dados do Sentinel não pode gravar no sistema de arquivos para arquivar dados. Para habilitar esse recurso, edite o arquivo init<SIDOracle>.ora do banco de dados.

Observação: Por padrão, o instalador define todos os tablespaces como autogrow (crescimento automático). Por padrão, o tamanho de crescimento de arquivo é 200 MB, mas o tamanho de arquivo máximo depende do valor fornecido durante a instalação.

Para permitir que o Oracle realize uma gravação no diretório de arquivamento:

1. Efetue login na máquina do banco de dados.
2. Navegue para o diretório $ORACLE_HOME/dbs.
3. Abra o arquivo init`<SIDOracle>.ora` em um editor de texto.

4 Edite o parâmetro UTL_FILE_DIR para especificar o caminho do diretório no qual os dados do Sentinel arquivados devem ser gravados. Você deve ter um dos seguintes:
   - UTL_FILE_DIR = *

     ou
   - UTL_FILE_DIR = [caminho de diretório específico]
5 Grave o arquivo e saia.

3.8.3 Serviço do Coletor

Durante a instalação do Serviço de Coletor, será configurado um coletor chamado Coletor Geral. Por padrão, a taxa de criação de eventos é de 5 eventos por segundo (eps). Esse Coletor pode ser usado para testar a instalação. Coletores adicionais podem ser transferidos por download a partir dosite da Novell na web (http://support.novell.com/products/sentinel/collectors.html).

3.8.4 Atualizando a chave de licença (da chave de avaliação à chave de produção)

Se você adquirir o produto após a avaliação, siga o procedimento abaixo para atualizar sua chave de licença no sistema e evitar a reinstalação.

Para atualizar a chave de licença (UNIX):

1 Efetue login na máquina em que o componente DAS está instalado como usuário do sistema operacional do Administrador do Sentinel (o padrão é esecadm).
2 No prompt de comando, mude o diretório para $ESEC_HOME/bin
3 Especifique o seguinte comando:
   ```
   ./softwarekey.sh
   ```
4 Digite o número 1 para definir sua chave principal. Pressione Enter.

Para atualizar a chave de licença (Windows):

1 Efetue login na máquina em que o componente DAS está instalado como usuário com direitos administrativos.
2 No prompt de comando, mude o diretório para %ESEC_HOME%\bin
3 Especifique o seguinte comando:
   ```
   .\softwarekey.bat
   ```
4 Digite o número 1 para definir sua chave principal. Pressione Enter.

3.8.5 Iniciando o serviço do Gerenciador de Coletor

Para iniciar o serviço do Gerenciador de Coletor:

1 Inicie o Sentinel 6.1
2 Clique na guia Admin > Tela de Servidores. Você também pode clicar em Tela de Servidores no painel Navegador.
3 Expanda a Tela de Servidores. É exibida uma lista de processos.

Clique o botão direito do mouse no Gerenciador de Coletor a ser iniciado e selecione Ações > Iniciar.

Ou

1. Inicie o Sentinel 6.1
2. Clique em Gerenciamento de Fonte de Eventos > Live View.
3. Na janela Gerenciamento de Fonte de Eventos (Live View), clique o botão direito do mouse no Gerenciador de Coletor a ser iniciado e selecione Iniciar.

3.8.6 Gerenciando o tempo

A Novell recomenda que todos os componentes do Sentinel, principalmente as máquinas do Mecanismo de Correlação e do Gerenciador de Coletor, sejam conectados a um Servidor NTP (Network Time Protocol) ou a outro tipo de Servidor de Horário. Se o horário do sistema não estiver sincronizado nas máquinas, o Mecanismo de Correlação do Sentinel e as Telas Ativas não funcionarão corretamente. Os eventos dos Gerenciadores de Coletor não serão considerados eventos em tempo real e, portanto, serão enviados diretamente para o banco de dados do Sentinel, ignorando os Sentinel Control Centers e os Mecanismos de Correlação.

Por padrão, o limite de dados em “tempo real” é de 120 segundos. Para modificar esse padrão, mude o valor de `esecurity.router.event.realtime.expiration` no arquivo `event-router.properties`. O horário de eventos do Sentinel é preenchido de acordo com o Horário do Dispositivo de Confiança ou com o Horário do Gerenciador de Coletor. Você pode selecionar o Horário do Dispositivo de Confiança ao configurar um coletor. O Horário do Dispositivo de Confiança é o horário em que o registro foi gerado pelo dispositivo e o Horário do Gerenciador de Coletor é o horário local do sistema Gerenciador de Coletor.

3.8.7 Modificando os scripts dbstart e dbshut da Oracle

O Sentinel não pode iniciar o banco de dados Oracle 10 devido a erros nos scripts `dbstart` e `dbshut` da Oracle. Para obter detalhes sobre os erros de script, consulte https://metalink.oracle.com (https://metalink.oracle.com) para obter os erros número 336299.1 com o assunto “dbstart errors out when executing in 10.2.0.1.0” (“erros dbstart ao executar no 10.2.0.1.0”), 5183726 e 4665320.

Após instalar o Sentinel 6, você precisará modificar os scripts `dbstart` e `dbshut` para o Sentinel iniciar um banco de dados Oracle 10.

Para modificar o script dbstart no Solaris 10:

1. Abra o script `dbstart` para edição no caminho $ORACLE_HOME/bin/dbstart.
2. Vá para a linha 78 e substitua-o por ORACLE_HOME_LISTNER=$ORACLE_HOME.
3. Adicione `#!/bin/bash` ao iniciar para solicitar o shell bash.
4. Verifique se “ORATAB” está apontando para ORATAB=/var/opt/oracle/oratab.

   Observação: Se ORATAB não estiver no local especificado acima, modifique o caminho de ORATAB manualmente para que ele corresponda ao local exato.

5. Grave e saia.
6. Para modificar o script dbshut no Solaris 10:

7 Abra o script dbshut para edição no caminho $ORACLE_HOME/bin/dbshut.

8 Verifique se “ORATAB” está apontando para ORATAB=/var/opt/oracle/oratab.

Observação: Se ORATAB não estiver no local especificado acima, modifique o caminho de ORATAB manualmente para que ele corresponda ao local exato.

---

9 Grave e saia.

Para modificar o script dbstart no RedHat Linux ES4:

1 Abra o script `dbstart` para edição no caminho $ORACLE_HOME/bin/dbstart.

2 Verifique se “ORATAB” está apontando para ORATAB=/etc/oratab.

Observação: Se ORATAB não estiver no local especificado acima, modifique o caminho de ORATAB manualmente para que ele corresponda ao local exato.

---

3 Grave e saia.

4 Para modificar o script dbshut no RedHat Linux ES4:

5 Abra o script `dbshut` para edição no caminho $ORACLE_HOME/bin/dbshut.

6 Verifique se “ORATAB” está apontando para ORATAB=/etc/oratab.

Observação: Se ORATAB não estiver no local especificado acima, modifique o caminho de ORATAB manualmente para que ele corresponda ao local exato.

---

7 Grave e saia.

Configuração do Advisor

4

Esta seção aborda como carregar dados do Advisor, como configurar atualizações regulares para os dados do Advisor e como configurar o Sentinel para executar relatórios do Advisor (fornecidos pela Novell) a partir da guia Advisor do Sentinel Control Center.

4.1 Visão geral do Advisor

O Advisor é um serviço de inscrição opcional que fornece correlação no nível do dispositivo entre eventos em tempo real de detecções de intrusão e sistemas de prevenção e resultados de exploração de vulnerabilidades da empresa. Ao fornecer informações de ataque normalizadas, o Advisor atua como um serviço de aviso prévio de detecção de ataques contra sistemas vulneráveis ("detecção de exploração"). Ele também fornece informações sobre correções associadas.

Observação: A instalação do Advisor é opcional. Porém, ele será um componente necessário se você quiser usar os recursos de Detecção de Exploração do Sentinel ou de Gerador de Relatórios do Advisor. O Advisor é um serviço de dados baseado em inscrição e requer uma licença adicional da Novell.

Os sistemas suportados estão listados a seguir com os tipos de dispositivo associados (IDS para sistema de detecção de intrusão, VULN para scanners de vulnerabilidade e FW para firewall).

Tabela 4-1 *Sistemas suportados e tipos de dispositivo associados*

Sistemas Suportados	Tipo de Dispositivo	Valor RV31
Cisco Secure IDS	IDS	Segura
Enterasys Dragon Host Sensor	IDS	Dragon
Enterasys Dragon Network Sensor	IDS	Dragon Network
Intrusion.com (SecureNet_Provider)	IDS	SecureNet_Provider
ISS BlackICE PC Protection	IDS	BlackICE
ISS RealSecure Desktop	IDS	RealSecure Desktop
ISS RealSecure Network	IDS	RealSecure
ISS RealSecure Server	IDS	RealSecure Server
ISS RealSecure Guard	IDS	RealSecure Guard

Sistemas Suportados	Tipo de Dispositivo	Valor RV31
Sourcefire Snort/Phalanx	IDS	Snort
Symantec Network Security 4.0 (ManHunt)	IDS	ManHunt
Symantec Intruder Alert	IDS	Intruder
McAfee IntruShield	IDS	IntruShield
eEYE Retina	VULN	Retina
Foundstone Foundscan	VULN	Foundstone
ISS Database Scanner	VULN	Database Scanner
ISS Internet Scanner	VULN	Internet Scanner
ISS System Scanner	VULN	System Scanner
ISS Wireless Scanner	VULN	Wireless Scanner
Nessus	VULN	Nessus
nCircle IP360	VULN	nCircle IP360
Qualys QualysGuard	VULN	QualysGuard
Cisco IOS Firewall	FW	Cisco IOS

Para habilitar a detecção de exploração total, os Coletores do Sentinel devem preencher corretamente diversas variáveis. Os coletores criados pela Novell preenchem essas variáveis por padrão.

- No coletor IDS, RV39 (MSSPCustomerName) deve ser definido como o Nome do Cliente do MSSP.
- Em coletores de vulnerabilidade e IDS, a variável RV31 (valor reservado) deve ser definida como o valor exibido na coluna RV31 acima. Essa string faz distinção entre maiúsculas e minúsculas.
- No coletor IDS, o DIP (IP de destino) deve ser preenchido com o endereço IP da máquina que está sendo atacada.
- No coletor IDS, o RT1 (DeviceAttackName) deve ser definido como o nome ou o código do ataque para esse IDS.

Os coletores fornecidos pela Novell definem essas variáveis por padrão.

4.2 Sobre a instalação do Advisor

Os dois componentes principais da instalação do Advisor são a configuração das atualizações regulares incluídas no serviço de inscrição de dados e o carregamento do conjunto inicial de dados do Advisor.

Para carregar os dados iniciais, a Novell recomenda que você use o ISO do Advisor Core Data, disponível no portal de Atendimento ao Cliente (Customer Care) da Novell para clientes que adquiriram a inscrição de dados do Advisor. O instalador carregará aproximadamente 10 GB de dados. Se o instalador não carregasse esses dados, você precisaria transmiti-los pela rede usando o serviço de atualização regular.

Por padrão, os scripts que iniciam os downloads automáticos ficam desabilitados. Eles deverão ser habilitados depois que o Advisor Core Data for carregado.

O Advisor deve ser instalado na mesma máquina que o DAS (Serviço de Acesso a Dados). As atualizações regulares poderão ser feitas manual ou automaticamente, dependendo das opções selecionadas no instalador do Sentinel.

- **Independente:** atualizações manuais
- **Download Direto da Internet:** atualizações programadas e automáticas

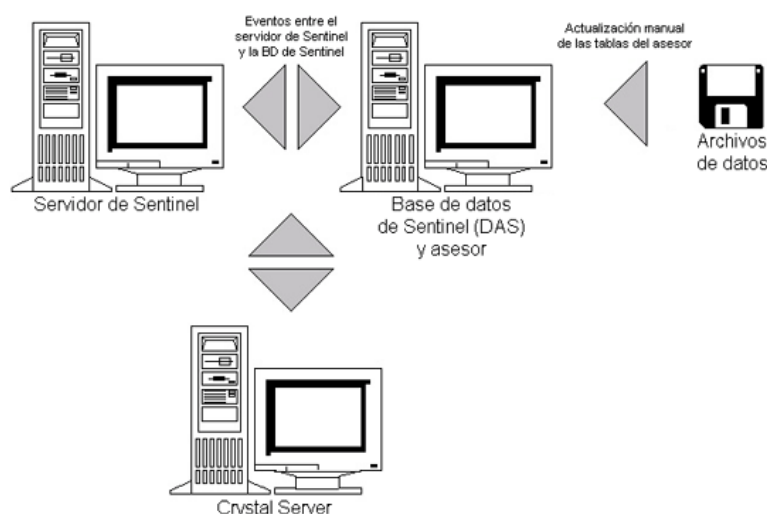
---

Observação: A alimentação de dados do Advisor para Sentinel 6.0 SP2 e versões posteriores foi ampliada com assinaturas adicionais. As mudanças no SP2 afetam o espaço de armazenamento necessário e os procedimentos de instalação.

A Novell recomenda aproximadamente 50 GB de espaço em disco para dados do Advisor, além do espaço em disco necessário para os dados do próprio Sentinel.

4.2.1 Configuração Independente

Na instalação Independente, o Advisor é um sistema isolado que exige atualização manual para seus dados. Freqüentemente, as instalações do Advisor em ambientes seguros não possuem conexão com a Internet e, portanto, exigem configuração independente.

Figura 4-1 *Configuração Independente*

Na configuração independente, os dados do Advisor podem ser transferidos por download manualmente de um destes locais:

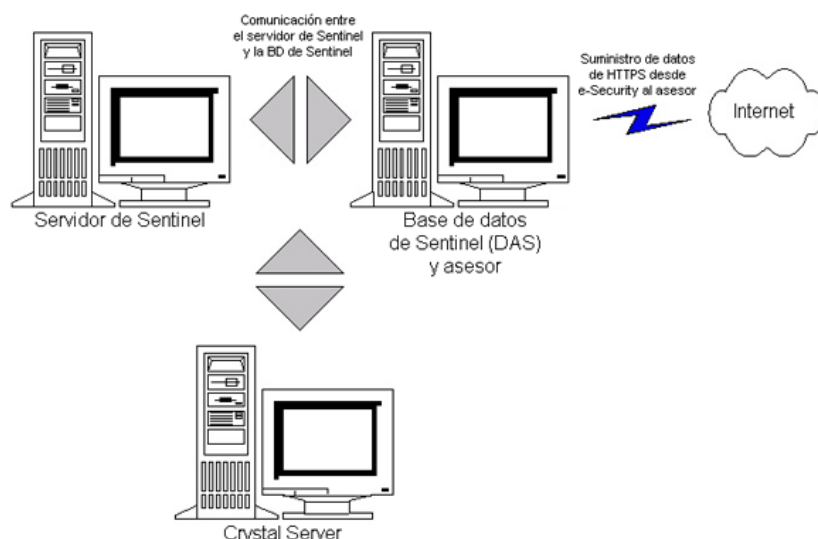
- Sentinel 6.0 SP1 e versões anteriores:

  https://advisor.novell.com/advisordata/ (https://advisor.novell.com/advisordata/)
- Sentinel 6.0 SP2 e versões posteriores:

  https://secure-www.novell.com/sentinel/advisor/advisordata (https://secure-www.novell.com/sentinel/advisor/advisordata)

4.2.2 Configuração de Download Direto da Internet

Na instalação de Download Direto da Internet, a máquina do Advisor está diretamente conectada à Internet. Nessa configuração, as atualizações dos dados do Advisor são transferidas por download automaticamente pela Internet em horários regulares (a cada 6 ou 12 horas). Para obter mais informações, consulte o Capítulo 3, "Instalando o Sentinel 6.1" na página 31.

Figura 4-2 *Download Direto da Internet*

4.3 Instalando o Advisor

Você pode instalar o Advisor quando instalar o Sentinel ou como um componente adicional.

Observação: A configuração do Advisor mudo significativamente entre o Sentinel 6.0 SP1 e o 6.0 SP2. Se estiver usando o 6.0 SP1 ou versões anteriores, consulte a versão apropriada da documentação em http://www.novell.com/documentation/sentinel6. (http://www.novell.com/documentation/sentinel6.)

Para instalar o Advisor:

1. Efetue login como usuário root no Solaris/Linux ou usuário administrador no Windows.
2. Insira e monte o CD de instalação do Sentinel.

3 Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e

- No Windows, execute `setup.bat`
- No Solaris/Linux:

  Para o modo de interface gráfica:

  `./setup.sh`

  Para o modo baseado em texto ("console serial"):

  `./setup.sh -console`

4 Selecione o idioma e clique em OK

5 Depois de ler a tela de boas-vindas, clique em Avançar.

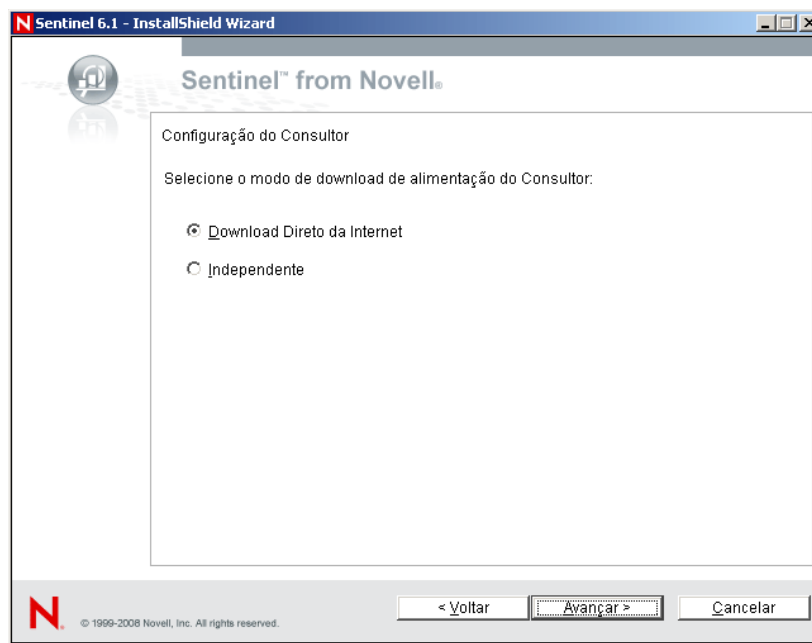
6 Leia e aceite o Contrato de Licença de Usuário Final e clique em Avançar.

7 Aceite o diretório de instalação padrão ou clique em Procurar para especificar o local da instalação. Clique em Avançar.

8 Selecione Personalizado. Clique em Avançar.

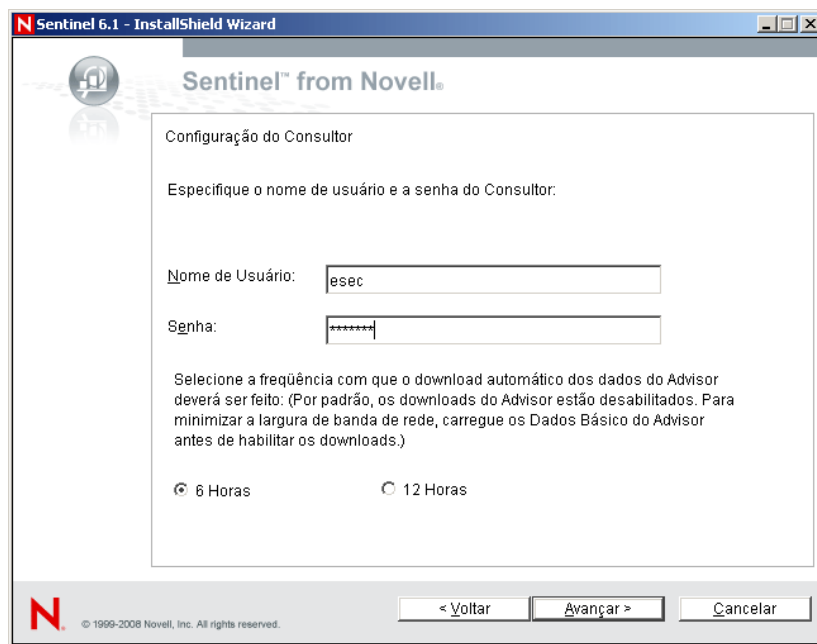
9 Nessa janela, forneça as informações de configuração e clique em Avançar.

- Número de Série
- Chave de Licença
- Senha do Sistema Global
- A senha que você digitar aqui será válida para todos os usuários padrão. Isso inclui o usuário do Administrador do Sentinel e os usuários do banco de dados. Para obter mais informações sobre a lista de usuários de banco de dados padrão criados com a instalação, consulte a Seção 3.8.2, “Banco de Dados do Sentinel” na página 58.

10 Selecione uma das duas opções disponíveis: Download Direto da Internet ou Independente.

11 Se tiver selecionado Download Direto da Internet, especifique o seguinte:

- Nome de usuário do Advisor

- Senha do Advisor
- Freqüência de atualização dos dados do Advisor

Observação: No Sentinel 6.0 SP2 e em versões posteriores, o nome de usuário e a senha do Advisor são o eLogin da Novell associado à compra do Advisor. Esse login pode ou não ser igual ao eLogin da Novell associado à compra do Sentinel. Para obter mais informações, consulte a seção "Guia Advisor" no *Guia do Usuário do Sentinel*.

12 Clique em Avançar.

Importante: Se seu nome de usuário e sua senha não puderem ser confirmados, você será solicitado a informar se deseja continuar.

No Sentinel 6.0 SP2 e em versões posteriores, o login e a senha devem ser o login e a senha da Novell associados aos direitos do Advisor. Um erro comum é inserir um login e uma senha da Novell incorretos; os dados podem até ser válidos, mas não estão associados aos direitos nem à licença do Advisor.

13 Clique em Instalar.

14 Após a instalação, você será solicitado a reinicializar o sistema ou a efetuar outro login e a iniciar os Serviços do Sentinel manualmente. Clique em Concluir para reinicializar o sistema.

Importante: O download programado do Advisor só funcionará após a reinicialização do sistema.

Dica: Após a instalação, para mudar os endereços de e-mail do Advisor, edite o arquivo `advisor_client.xml` no diretório $ESEC_HOME/config. Para obter mais informações, consulte a "Guia Advisor" no *Guia do Usuário do Sentinel*.

4.3.1 Carregando dados

Embora você possa executar o carregamento inicial de dados do Advisor usando o serviço programado (Download Direto da Internet) ou manualmente, usando a opção Independente, essa abordagem não é recomendada devido à carga de rede. Portanto, por padrão, os scripts `advisor.sh` e `advisor.bat` inicialmente ficam desabilitados. Habilite-os após o carregamentos dos dados usando a Detecção de Exploração e o Advisor Core Data do Sentinel 6. O disco do Advisor Core Data contém um instantâneo dos dados do Advisor. O carregamento desses dados reduz significativamente a quantidade de tempo e a largura de banda de rede necessários para atualizar o banco de dados.

O Advisor Core Data está disponível no portal do Atendimento ao Cliente (Customer Care) da Novell para clientes que tenham adquirido uma assinatura anual do Advisor. O ISO tem menos de 900 MB, mas carrega aproximadamente 10 GB de dados nas tabelas do Advisor.

O carregamento inicial de dados pode levar até um dia para ser concluído, dependendo das especificações das máquinas e de outros carregamentos do servidor de banco de dados.

Após o carregamento inicial de dados, atualizações incrementais poderão ser carregadas manualmente ou por meio do recurso de Download Direto da Internet.

Importante: O instalador de dados do Advisor só funcionará com o Sentinel 6.0 SP2 e versões posteriores depois que os patches de banco de dados apropriados forem aplicados como parte do processo de instalação de patches. O processo de upgrade e o instalador de dados substituirão todos os dados do Advisor transferidos por download antes do Sentinel 6.0 SP2.

Para fazer download de instantâneos de dados do Advisor:

1. Efetue login como usuário root no Solaris/Linux ou usuário administrador no Windows.
2. Insira e monte o disco de instalação do Sentinel 6 Advisor Core Data.
3. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e
   - No Solaris/Linux, execute `advisor_bcp_in.sh`
   - No Windows, execute `advisor_bcp_in.bat`
4. No console, forneça as credenciais de banco de dados adequadas:
   - No Linux, forneça o nome de usuário do banco de dados (o padrão é esecdba), a senha e o SID Oracle (nome da instância).
   - No Windows, forneça o nome de host do banco de dados, o nome do banco de dados (o padrão é ESEC) e o modo de autenticação do banco de dados. Se usar a Autenticação do SQL, forneça também o nome de usuário do banco de dados (o padrão é esecdba) e a senha.
5. Especifique o tempo de pausa, em segundos, entre o processamento de cada arquivo. O padrão é 0 segundo, mas, se a carga do banco de dados for alta, você poderá aumentar esse valor para introduzir uma pausa entre o processamento dos arquivos de dados.
6. Para aumentar a eficácia do processo de carregamento de dados, o sistema desabilita índices e restrições nas tabelas do Advisor e trunca essas tabelas. A seguinte mensagem é exibida:

   ```
   Disabling indexes on the Advisor tables…
   Successfully disabled indexes on the Advisor tables
   Disabling constraints on the Advisor tables...
   ```

```
Successfully disabled constraints on the Advisor tables
Truncating Advisor tables...
Successfully truncated Advisor tables
```

7 O script do Advisor é iniciado e as tabelas apropriadas são alimentadas com os dados em massa. O instantâneo dos dados é armazenado no banco de dados.

8 Depois que todos os arquivos do instantâneo forem carregados, o sistema habilitará restrições, recriará índices e exibirá as seguintes mensagens:

```
Successfully enabled constraints on the Advisor tables
Successfully rebuilt indexes on the Advisor tables
```

9 Quando a alimentação em massa for concluída, o sistema exibirá uma mensagem de êxito.

10 Habilite as atualizações incrementais de dados do Advisor.

Atualizações incrementais e regulares dos dados do Advisor devem ser planejadas (programadas com o Download Direto da Internet ou realizadas manualmente por meio da opção Independente) para atualizar e manter atualizado o banco de dados do Advisor.

4.3.2 Habilitando atualizações do Advisor

Para evitar que a rede seja sobrecarregada, os downloads incrementais do Advisor ficam desabilitados por padrão. Eles deverão ser habilitados depois que o Advisor Core Data for carregado.

Para habilitar os downloads do Advisor:

1 Abra o arquivo `advisor.sh` ou `advisor.bat` para edição.

   No Linux: $ESEC_HOME/bin/advisor.sh

   No Windows: %ESEC_HOME%\bin\advisor.bat

2 **Para Linux:**

   Coloque um sinal de tralha (#) na frente do comando exit no começo do arquivo para comentá-lo.

```
# exit
```

   Para Windows:

   Digite rem na frente do comando exit no começo do arquivo para comentá-lo.

```
rem exit
```

3 Grave o arquivo.

O próximo download manual ou programado deverá carregar dados conforme o esperado.

4.3.3 Conectando-se ao Advisor Server por meio de um proxy

Para se conectar ao Advisor Server por meio de um servidor proxy para fazer downloads de alimentação, você deve atualizar a configuração do Advisor. Isso poderá exigir a inclusão de até quatro novas propriedades em cada arquivo `container.xml` usado pelo Advisor. Se o servidor proxy não exigir autenticação, você só precisará adicionar as informações de porta e host desse servidor. Se o servidor proxy exigir autenticação, você precisará adicionar o nome de usuário e a senha desse servidor.

Para configurar o Advisor:

1. Instale o Advisor no modo "Conexão Direta". Como o instalador atual não suporta conexão por servidor proxy, ocorrerá falha na verificação de autenticação executada pelo instalador. Continue com a instalação mesmo assim.
2. Procure a pasta `%ESEC_HOME%\sentinel\config`.
3. Abra `advisor_client.xml` e adicione as seguintes linhas à seção DownloadComponent.

   ```
   <property name="proxy_host">proxyHost</property>
   <property name="proxy_port">proxyPort</property>
   ```

   Adicione também as propriedades a seguir se o servidor proxy exigir autenticação.

   ```
   <property name="proxy_username">proxyUser</property>
   <property name="proxy_password" />
   ```
4. Se o servidor proxy exigir autenticação, siga estas etapas:
   - Copie o arquivo `proxy_password_update.bat` para a pasta %ESEC_HOME%\sentinel\bin.
   - Para atualizar os arquivos de container do Advisor com a senha do usuário proxy, execute o seguinte comando:
     `%ESEC_HOME%\sentinel\bin\proxy_password_update.bat proxyPasswd`
   - Verifique se agora o `advisor_client.xml` contém a senha de proxy criptografada.
5. Execute `advisor.bat` para fazer download dos dados do Advisor e processá-los. Para verificar se o Advisor pode se conectar por meio do servidor proxy, examine os seguintes arquivos de registro: `%ESEC_HOME%\sentinel\log\Advisor_0.0.log` e `%ESEC_HOME%\sentinel\log\advisor.log`.

4.4 Relatórios do Advisor

Crystal Reports Server™ é a ferramenta de geração de relatórios integrada ao Sentinel.

Para executar o Crystal Reports no Advisor:

- Instale e configure o Crystal Server. Para obter mais informações sobre a instalação do Crystal Reports Server, consulte o Capítulo 8, "Crystal Reports para Windows" na página 97 e o Capítulo 9, "Crystal Reports para Linux" na página 127.
- Publique Crystal Reports do Advisor no Crystal Server.

4.4.1 Configuração de relatórios do Advisor

Para executar relatórios do Advisor, siga as etapas de configuração do Crystal Reports Server para Windows ou Linux e configure o URL do Advisor para relatórios. Para obter mais informações sobre como importar gabaritos de relatórios e configurar o Sentinel Control Center para mostrar os relatórios do Advisor, consulte Capítulo 8, "Crystal Reports para Windows" na página 97 e Capítulo 9, "Crystal Reports para Linux" na página 127.

4.5 Fazendo a manutenção do Advisor

Diversas tarefas de manutenção do Advisor são descritas no guia do usuário do Sentinel:

- Atualização manual dos dados do Advisor: Para serem efetivos, os dados do Advisor devem ser atualizados regularmente, à medida que novos ataques e vulnerabilidades são incluídos na alimentação de dados. Se não forem programadas com o Download Direto da Internet, essas atualizações deverão ser executadas manualmente.
- Mudança da senha usada pelo Advisor para atualizações automáticas de dados, se necessário
- Mudança da configuração dos e-mails de notificação do Advisor
- Mudança do horário programado de atualização de dados

Para obter mais informações sobre todas essas tarefas de manutenção, consulte “Fazendo a manutenção do Advisor” no *Guia do Usuário do Sentinel*.

Testando a instalação

5

5.1 Testando a instalação

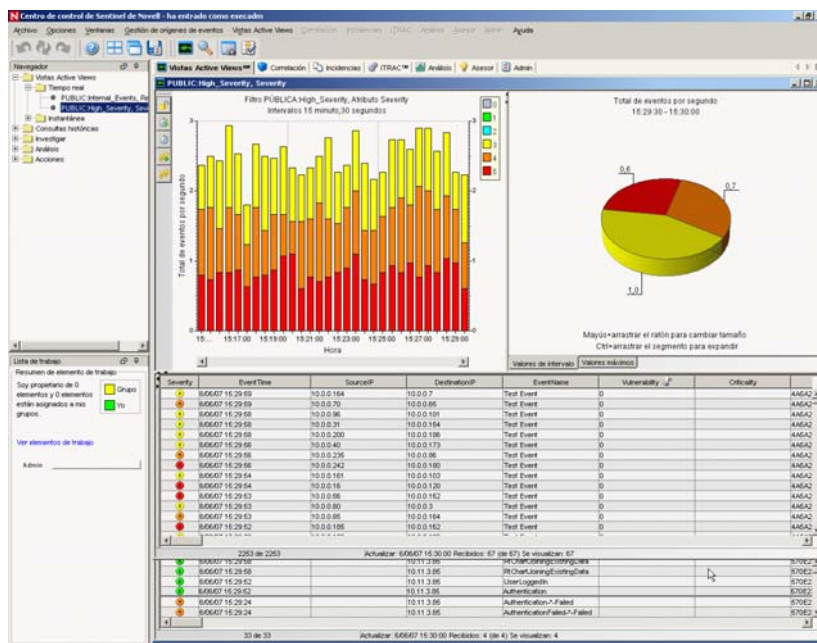
O Sentinel é instalado com um Coletor de demonstração que pode ser usado para testar muitas das funções básicas do sistema. Usando esse coletor, você pode testar Telas Ativas, a criação de incidentes, regras de correlação e relatórios. O procedimento a seguir descreve as etapas que você deve seguir para testar o sistema e mostra os resultados esperados. Talvez você não veja exatamente os mesmos eventos, mas seus resultados deverão ser semelhantes aos resultados abaixo.

No nível básico, esses testes permitem que você verifique se:

- Os Serviços do Sentinel estão ativos
- A comunicação pelo barramento de mensagem é funcional
- Os eventos de auditoria interna estão sendo enviados
- Os eventos podem ser enviados de um Gerenciador de Coletor
- Os eventos estão sendo inseridos no banco de dados e podem ser recuperados por meio da Consulta de Eventos do Histórico ou do Crystal Reports
- Os Incidentes podem ser criados e vistos
- O Mecanismo de Correlação está avaliando regras e acionando os eventos correlacionados
- O Gerenciador de Dados do Sentinel pode se conectar ao banco de dados e ler as informações de partição

Se um desses testes falhar, revise o registro de instalação e outros arquivos de registro e entre em contato com o Suporte Técnico da Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup), se necessário.

Para testar a instalação:

1 Clique duas vezes no ícone do Sentinel Control Center na área de trabalho.
2 Efetue login no sistema utilizando o Usuário Administrativo do Sentinel especificado durante a instalação (o padrão é esecadm). O Sentinel Control Center é aberto e a guia Telas Ativas é exibida com os eventos filtrados pelos filtros públicos “Internal_Events” e “High_Severity”.

3 Vá para o menu Gerenciamento de Fonte de Eventos e escolha Live View.

4 Em Formato de Gráfico, clique o botão direito do mouse na fonte de evento 5 eps e selecione Iniciar.

5 Feche a janela Live View do Gerenciamento de Fonte de Eventos.

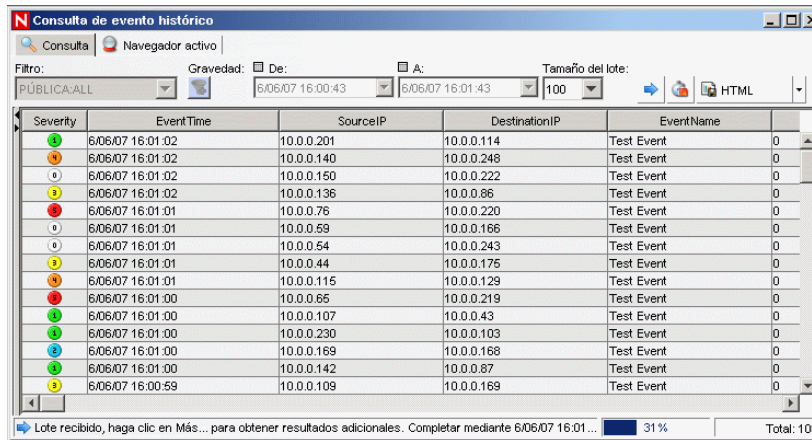
6 Vá para a guia Telas Ativas. Haverá uma janela ativa chamada PUBLIC: High_Severity, Severity. Pode levar algum tempo para que o coletor seja iniciado e os dados sejam exibidos nessa janela.

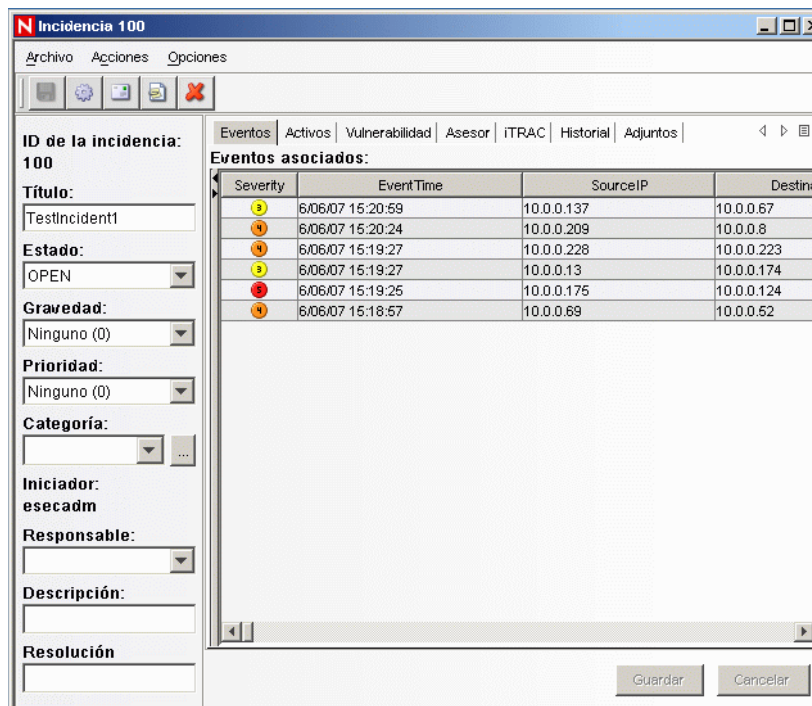
7 Clique no botão Consulta de Eventos na barra de ferramentas. A janela Consulta de Eventos do Histórico é exibida.

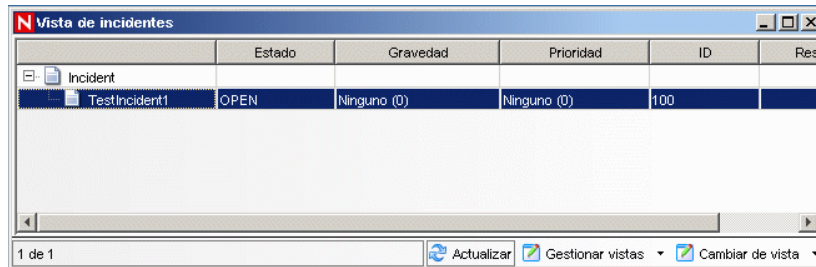
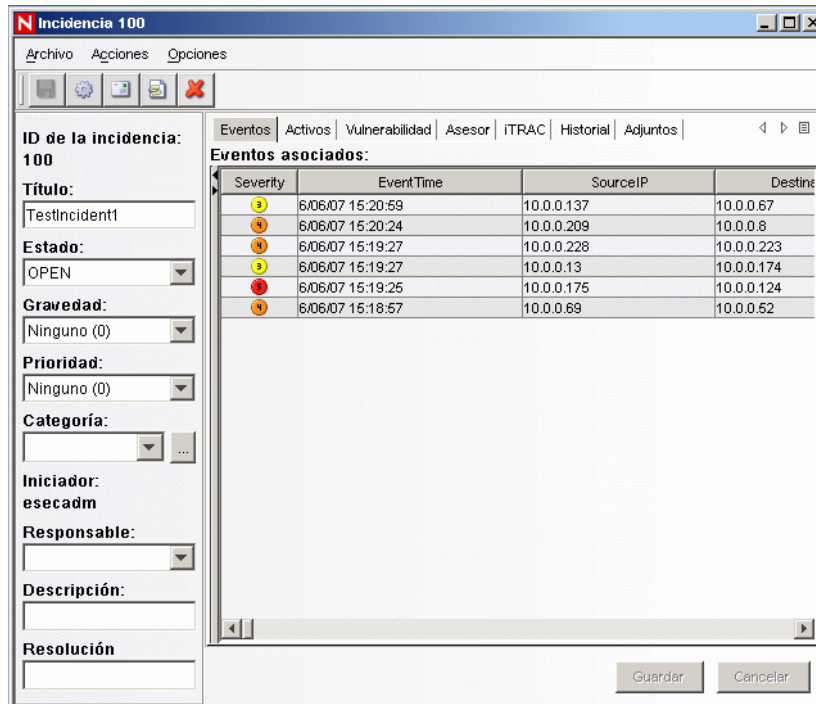
8 Na janela Consulta de Eventos do Histórico, clique na seta para baixo do Filtro para selecionar o filtro desejado. Realce Público: Todos os filtros e clique em Selecionar.

9 Selecione um horário que abranja o horário em que o Coletor ficou ativo. Selecione o intervalo de datas usando as setas suspensas dos campos De e Até.

10 Selecione um tamanho de lote no menu suspenso Tamanho do lote.

11 Clique no ícone da lupa para executar a consulta.

12 Mantenha a tecla Crtl ou Shift pressionada e selecione vários eventos na janela Consulta de Eventos do Histórico.

13 Clique o botão direito do mouse e selecione Criar Incidente.

14 Nomeie o incidente como TestIncident1 e clique em Criar. É exibida uma notificação de êxito. Clique em OK.

15 Vá até a guia Incidente. O Gerenciador de Telas de Incidentes é exibido. No Gerenciador de Telas de Incidentes você verá o incidente que acabou de criar.

16 Clique duas vezes no incidente para exibi-lo.

17 Feche a janela do incidente. Vá para Arquivo > Sair ou clique no "X" no canto superior direito da janela.

18 Clique na guia Análise. No Navegador de Análise, abra a pasta Eventos.

19 Clique em Consultas de Eventos do Histórico.

20 Clique em Análise > Criar Relatório ou clique no ícone Criar Relatório. A janela Consulta de Eventos é exibida. Defina o seguinte:

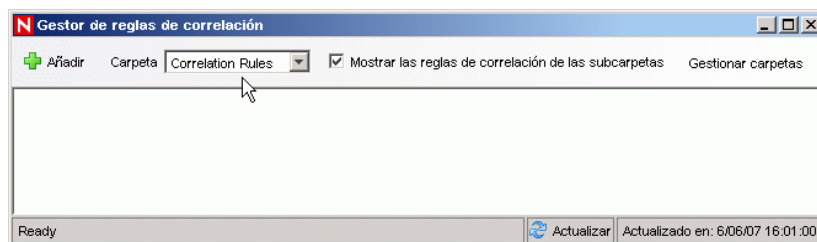
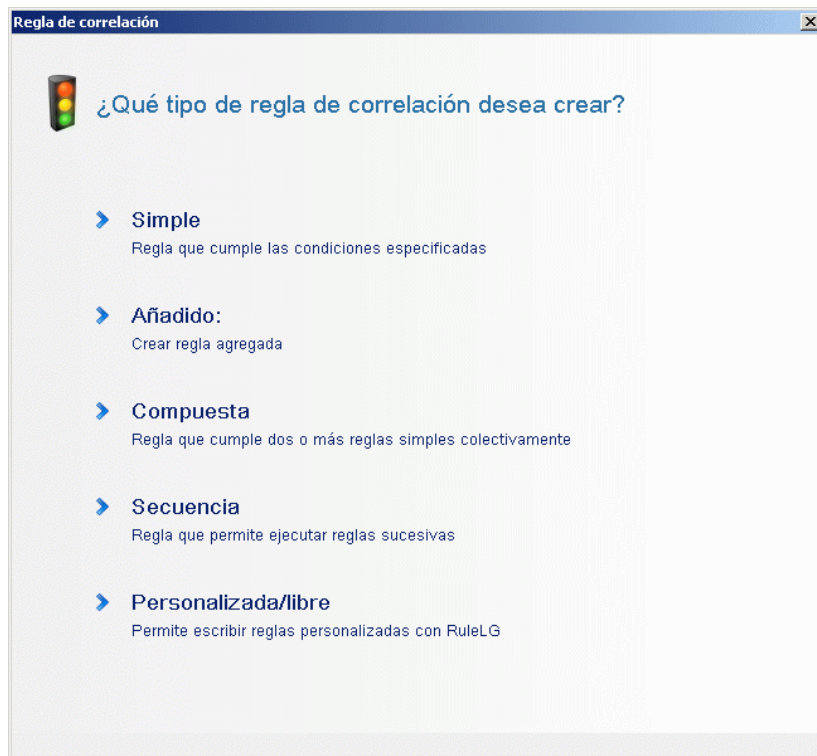
- espaço de tempo
- filtro
- nível de severidade
- tamanho do lote (este é o número de eventos a ver – eventos exibidos dos mais antigos para os mais recentes)

21 Clique no ícone Iniciar a pesquisa.

22 Para ver o próximo lote de eventos, clique em Mais.

23 Reorganize as colunas arrastando-as e soltando-as, e organize a ordem de classificação clicando no cabeçalho da coluna.

24 Quando sua consulta estiver completa, ela será adicionada à lista de consultas rápidas do navegador.

25 Vá para a guia Correlação. O Gerenciador de Regras de Correlação é exibido.

26 Clique em Adicionar. O Assistente de Regras de Correlação é exibido.

27 Clique em Simples. A janela Regra Simples é exibida.

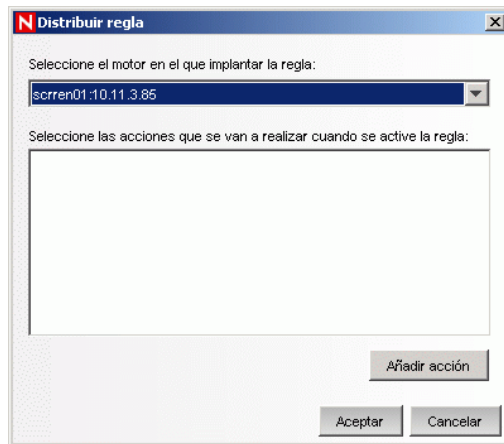
28 Use os menus suspensos para definir os critérios como Severity=4. Clique em Avançar. A janela Atualizar Critérios é exibida.

29 Selecione Não executar ações sempre que esta regra acionar a próxima e use o menu suspenso para definir o período como 1 minuto. Clique em Avançar. A janela Descrição Geral é exibida.

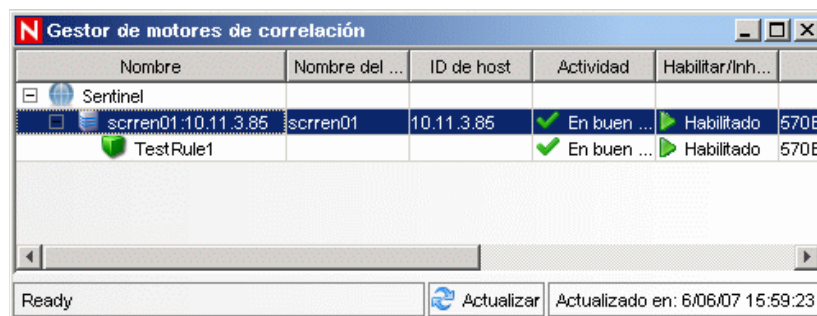
30 Nomeie a regra como “Regra de Correlação”, forneça uma descrição e clique em Avançar.

31 Selecione “Não, não criar outra regra” e clique em Avançar.

32 Abra a janela Gerenciador de Regras de Correlação.

33 Realce uma regra e clique no link Implantar regras. A janela Implantar Regras é exibida.

34 Na janela Implantar Regras, selecione na lista suspensa o mecanismo a ser usado na implantação da regra.

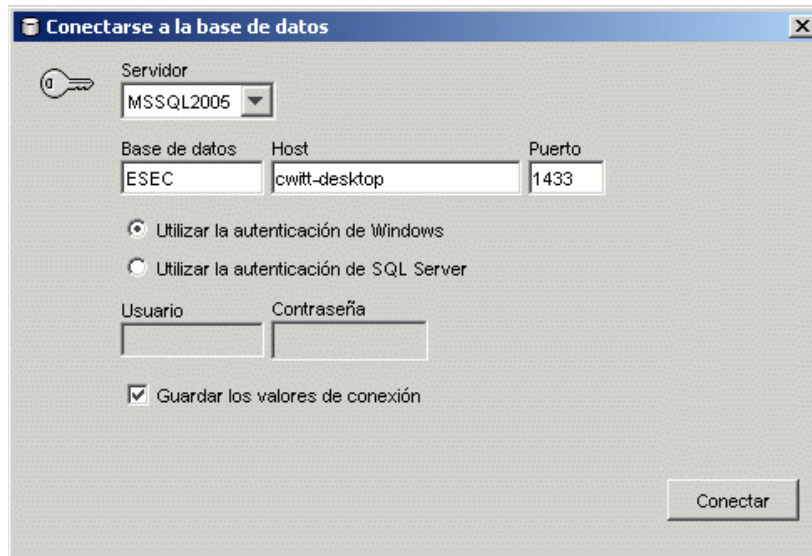
35 Selecione a ação Enviar E-mail para associá-la à regra e clique em OK. Antes de associar uma ação, você deve criá-la no Sentinel.

36 Selecione o Gerenciador de Mecanismos de Correlação. No Gerenciador de Mecanismos de Correlação, é possível verificar se a regra está implantada/habilitada.

37 Vá para a guia Telas Ativas e verifique se o Evento Correlacionado foi gerado.

Severity	EventTime	SourceIP	DestinationIP	EventName	Vulnerability	
4	6/06/07 15:54:29	10.0.0.187	10.0.0.113	Test Event	0	4A5A
5	6/06/07 15:54:29	10.0.0.97	10.0.0.232	Test Event	0	4A5A
3	6/06/07 15:54:29	10.0.0.59	10.0.0.6	Test Event	0	4A5A
4	6/06/07 15:54:28	10.0.0.32	10.0.0.105	Test Event	0	4A5A
3	6/06/07 15:54:28	10.0.0.197	10.0.0.46	Test Event	0	4A5A
4	6/06/07 15:54:28	10.0.0.95	10.0.0.89	Test Event	0	4A5A
5	6/06/07 15:54:27	10.0.0.147	10.0.0.186	Test Event	0	4A5A
3	6/06/07 15:54:26	10.0.0.88	10.0.0.77	Test Event	0	4A5A
5	6/06/07 15:54:25	10.0.0.129	10.0.0.37	Test Event	0	4A5A
3	6/06/07 15:54:25	10.0.0.149	10.0.0.116	Test Event	0	4A5A
4	6/06/07 15:54:24	10.0.0.151	10.0.0.42	Test Event	0	4A5A
4	6/06/07 15:54:24	10.0.0.220	10.0.0.62	Test Event	0	4A5A
4	6/06/07 15:54:22	10.0.0.61	10.0.0.109	Test Event	0	4A5A

38 Feche o Sentinel Control Center.

39 Clique duas vezes no ícone do SDM (Gerenciador de Dados do Sentinel) na área de trabalho.

40 Efetue login no SDM usando o Usuário Administrativo do Banco de Dados especificado durante a instalação (o padrão é esecdba).

41 Clique em cada guia para verificar se você pode acessá-las.

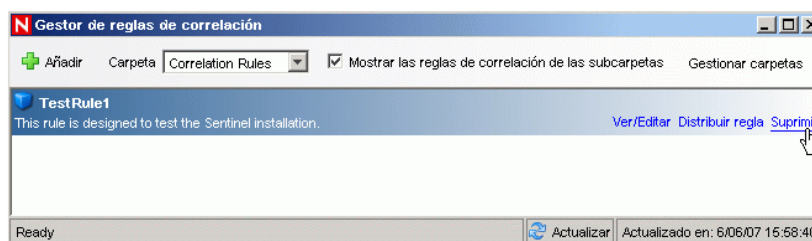
42 Feche o Gerenciador de Dados do Sentinel.

Se puder executar todas essas etapas sem erros, você terá concluído a verificação básica da instalação do sistema Sentinel.

5.2 Realizando limpeza após o teste

Depois de concluir a verificação do sistema, você deve remover os objetos criados para os testes.

Para realizar uma limpeza após o teste do sistema:

1. Efetue login no sistema utilizando o Usuário Administrativo do Sentinel especificado durante a instalação (o padrão é esecadm).
2. Vá para a guia Correlação.
3. Abra o Gerenciador de Mecanismos de Correlação.
4. Clique o botão direito do mouse em TestRule1 no Gerenciador de Mecanismos de Correlação e selecione Desfazer Implantação.
5. Abra o Gerenciador de Regras de Correlação.
6. Selecione TestRule1 e clique em Apagar.

7. Vá para o menu Gerenciamento de Fonte de Eventos e escolha Live View.
8. Na hierarquia gráfica de fontes de eventos, clique o botão direito do mouse em Coletor Geral e selecione Parar.
9. Feche a janela Gerenciamento de Fonte de Eventos.
10. Vá até a guia Incidentes.
11. Abra o Gerenciador de Telas de Incidentes.
12. Selecione TestIncident1, clique o botão direito do mouse e selecione Apagar.

5.3 Introdução

Para começar a utilizar dados reais, você precisará importar e configurar os Coletores apropriados para seu ambiente, configurar suas próprias regras, criar workflows iTRAC, e assim por diante. Os Sentinel Solution Packs podem ajudar você a começar rapidamente.

Adicionando componentes do Sentinel

6

6.1 Adicionando componentes do Sentinel a uma instalação existente

Às vezes, pode ser necessário instalar componentes do Sentinel adicionais em uma máquina que já possua uma instalação do Sentinel. Por exemplo, talvez você precise instalar o Construtor de Coletor em uma máquina em que o Sentinel Control Center já esteja instalado.

O instalador do Sentinel simplifica a execução desse tipo de instalação. Primeiramente, verifique se os pré-requisitos do componente adicional que está sendo instalado foram atendidos conforme especificado em Capítulo 3, “Instalando o Sentinel 6.1” na página 31. Os requisitos da máquina provavelmente aumentarão quando os componentes adicionais forem instalados. Em seguida, execute o instalador do Sentinel na máquina de destino como se estivesse realizando uma instalação em uma máquina “limpa”. Se estiver executando no modo adição de componente, o instalador mudará seu comportamento da seguinte maneira:

- O instalador detectará automaticamente a instalação do Sentinel existente e exibirá uma tela indicando a localização da instalação existente e quais componentes já estão instalados.
- O instalador não solicitará o diretório de destino. O diretório de destino da instalação existente será usado.
- A instalação não solicitará que você selecione o tipo de instalação Simples ou Personalizada. A instalação Personalizada será usada por padrão.

Observação: Só pode haver uma instância do Advisor e do Servidor de Comunicação em uma instalação distribuída do Sentinel.

6.2 Instalando nós de equilíbrio de carga adicionais

Ocasionalmente, pode ser necessário incluir um nó de processamento adicional no ambiente distribuído do Sentinel para equilibrar a carga nas máquinas. Por exemplo, se o uso de memória for alto em uma máquina que esteja executando o Mecanismo de Correlação, você poderá optar por adicionar outra máquina para executar o Mecanismo de Correlação. (Talvez seja necessário obter uma licença adicional.) Em seguida, você poderá implantar novamente as regras de correlação nesses dois mecanismos para reduzir a carga em uma máquina individual, caso todas as regras tenham sido implantadas nela.

Para fazer isso, basta executar o instalador na nova máquina, conforme descrito em Capítulo 3, “Instalando o Sentinel 6.1” na página 31. Ao executar as etapas do instalador, selecione apenas os componentes para os quais deseje incluir nós de equilíbrio de carga adicionais. É possível realizar o equilíbrio de carga nos seguintes componentes:

- Mecanismo de Correlação
- Gerenciador de Coletor
- Processo DAS_Binary

O processo DAS_Binary é responsável pela inserção de bancos de dados de eventos. Como inserções de bancos de dados de eventos podem representar um gargalo no fluxo de eventos, efetuar o equilíbrio de carga no processo DAS_Binary geralmente resulta em uma significativa melhora no desempenho, em termos de throughput de eventos por segundo. Além disso, você pode efetuar o equilíbrio de carga dos componentes Mecanismo de Correlação e Gerenciador de Coletor instalando instâncias desses componentes em máquinas adicionais.

6.2.1 Processos DAS_Binary múltiplos

Embora não seja um equilíbrio de carga verdadeiro, é possível configurar instâncias múltiplas do DAS_Binary e um sistema Sentinel para melhorar o desempenho. DAS_Binary é o processo que gerencia a inserção de eventos no banco de dados; as taxas de evento mais altas alcançadas pela Novell em testes internos foram obtidas com processos DAS_Binary múltiplos. Para obter mais informações sobre testes de desempenho, consulte o site de Documentação da Novell (http://www.novell.com/documentation/sentinel61).

Processos DAS_binary múltiplos podem ser instalados na mesma máquina ou distribuídos por várias máquinas.

Para configurar instâncias do processo DAS_binary em máquinas diferentes:

1. Use o instalador do Sentinel para instalar o componente DAS em cada uma das máquinas que executarão o processo DAS_Binary. Todos os processos DAS_Binary devem se conectar ao mesmo banco de dados; portanto, durante a instalação, forneça as mesmas informações de conexão de banco de dados fornecidas na instalação inicial do DAS.
2. Faça as seguintes modificações em todas as máquinas que executarão o DAS_Binary:

   2a Efetue login como esecadm (no UNIX) ou como Administrador (no Windows) em uma das máquinas que executarão uma instância do processo DAS_Binary e localize o arquivo `configuration.xml` no diretório $ESEC_HOME/config (%ESEC_HOME%\config no Windows).

   2b Adicione as seguintes informações à seção de serviços do arquivo `configuration.xml`:

   ```
   <service name="DAS_Binary_EventStore" plugins=""
   strategyid="sentinel_client" subscriptiongroup="dasbin" />
   ```

   2c Grave o arquivo `configuration.xml`.

3 Nas máquinas que estiverem executando processos DAS_Binary secundários, faça as modificações a seguir. Um DAS_Binary secundário é um DAS_Binary que não está sendo executado no Sentinel Server principal.

3a Remova o arquivo `sentinelhost.id` do diretório $ESEC_HOME/data (%ESEC_HOME%\data no Windows). Isso forçará o Gerenciador de Coletor dessa máquina a gerar um novo ID, em vez de usar o ID usado pelo Gerenciador de Coletor do Sentinel Server.

3b Os outros processos DAS devem ser desabilitados. Para isso, na seção de processos do arquivo `configuration.xml` das máquinas com DAS_Binary único, defina o atributo min_instances desta maneira:

```
min_instances=”0”
```

para as seguintes entradas de processo:

- DAS_RT
- DAS_Aggregation
- DAS_Query
- DAS_ITRAC

4 O serviço secundário do Sentinel deve ser usado. Portanto, o arquivo `sentinel.conf` contido no diretório ESEC_HOME/config deve ser modificado. Para modificá-lo, remova o caractere # do início desta linha para anular o comentário:

```
wrapper.app.parameter.1=../config/sentinel.xml
```

em seguida, insira o caractere # no início da linha a seguir para incluir um comentário:

```
#wrapper.app.parameter.1=../config/sentinel_primary.xml
```

5 Faça as seguintes mudanças no arquivo `das_binary.xml` contido em uma das máquinas que executarão um processo DAS_Binary:

5a Faça uma cópia do componente DispatchManager inteiro e mude o ID do novo componente de DispatchManager para EventStoreDispatchManager. Depois que você fizer essa mudança, um dos componentes terá o ID DispatchManager e o outro, o ID EventStoreDispatchManager. Veja o exemplo abaixo para saber qual deverá ser a aparência do novo componente EventStoreDispatchManager.

5b Atualize o valor da propriedade `esecurity.communication.service` do componente EventStoreDispatchManager para DAS_Binary_EventStore.

5c Remova a propriedade `handler:esecurity.event.create` do componente DispatchManager.

5d Remova todas as propriedades cujo nome comece com “handler:*”, exceto `handler:esecurity.event.create`, do componente EventStoreDispatchManager. A sub-rotina `handler:esecurity.event.create` deverá ser a única sub-rotina definida no componente EventStoreDispatchManager.

5e Adicione o seguinte elemento XML ao componente EventStoreService:

```
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

5f Grave o arquivo `das_binary.xml`.

6 Copie o arquivo `das_binary.xml` em todas as máquinas que executarão um processo DAS_Binary. Veja a seguir um exemplo retirado do arquivo `das_binary.xml` mostrando o componente EventStoreDispatchManager.

```
<obj-component id="EventStoreDispatchManager">
<class>esecurity.ccs.comp.dispatcher.CommDispatcherManager</class>
<property
name="esecurity.communication.service">DAS_Binary_EventStore</
property>
<property name="dependencies">DAS_Query</property>
<property
name="handler:esecurity.event.create">esecurity.ccs.cracker.EventC
racker@ewizard_binary_event,correlation_binary_event,database_bina
ry_event,database_tagged_event,correlation_binary_event_update</
property>
<obj-component id="DispatcherStatsService">
<class>esecurity.ccs.comp.dispatcher.stats.DispatcherStatsManager<
/class>
<property name="ReportIntervals">900,3600,14400,86400</property>
<property name="MinLogReportInterval">900</property>
<property name="MinPublishReportInterval">86400</property>
<property name="ReportByServiceName">true</property>
<property name="ReportByMethodName">true</property>
<obj-component-ref>
<name>EventPublisher</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
</obj-component>
</obj-component>
```

Veja a seguir um exemplo retirado do arquivo `das_binary.xml` mostrando o componente EventStoreService:

```
<obj-component id="EventStoreService">
<class>esecurity.ccs.comp.event.EventStoreService</class>
<property name="handler">esecurity.event.create</property>
<property name="waitBlocked">true</property>
<property name="maxThreads">6</property>
<property name="minThreads">6</property>
<property name="maxThreadsQueued">10</property>
<property name="queueSize">1000000</property>
<obj-component-ref>
<name>ThreadPool</name>
<ref-id>EventStoreThreadPool</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
<obj-component id="Persistor">
<class>esecurity.ccs.comp.event.jdbc.JDBCEventStore</class>
<property name="insert.batchsize">600</property>
```

```
<property
name="insert.strategy">esecurity.ccs.comp.event.jdbc.JDBCLoadStrat
egy</property>
<property name="insert.oci.workerCount">5</property>
<property name="insert.oci.queueWaitTime">1</property>
<property name="insert.oci.highWatermark">10000000</property>
<property name="insert.oci.lowWatermark">9000000</property>
<property name="insert.oci.optimizationFlag">on</property>
<property name="insert.pmaxWarningTime">300</property>
<property name="insert.pminWarningTime">300</property>
</obj-component>
<obj-component-ref>
<name>EventRedirect</name>
<ref-id>EventFileRedirectService</ref-id>
</obj-component-ref>
</obj-component>
```

7 Para ativar as mudanças, reinicie o serviço do Sentinel em todas as máquinas em que houve modificações.

No UNIX:

```
$ESEC_HOME/bin/sentinel.sh restart
```

No Windows:

```
Restart the "Sentinel" service using the Windows Service Manager.
```

Para configurar instâncias múltiplas do DAS_binary na mesma máquina:

1 Efetue login como esecadm (no UNIX) ou como Administrador (no Windows) na máquina que executará instâncias múltiplas do processo DAS_Binary e localize o arquivo `configuration.xml` no diretório $ESEC_HOME/config (%ESEC_HOME%\config no Windows).

2 No arquivo `configuration.xml`, localize a seção do arquivo xml que define as entradas de serviços (veja o exemplo a seguir). Faça uma cópia da entrada do serviço DAS_Binary para cada instância do DAS_Binary que deseja executar. Por exemplo, para executar dois processos DAS_Binary, faça duas cópias da entrada do serviço DAS_Binary. Apague o atributo uuid de todas as entradas de serviço (o atributo uuid será regenerado automaticamente quando o Sentinel for iniciado). Veja a seguir um exemplo de entrada do serviço DAS_Binary.

```
<service name="DAS_Binary" plugins="" strategyid="sentinel_client"
uuid="4DA52BE0-E7A4-1029-BB2F-00132168CBDF"/>
```

3 No arquivo `configuration.xml`, crie uma cópia do xml a seguir da entrada do serviço DAS_Binary_EventStore para cada instância do DAS_Binary a ser executada. Esse serviço não existe no arquivo `configuration.xml`, portanto, você deverá copiá-lo do exemplo abaixo. Por exemplo, para executar dois processos DAS_Binary, faça duas cópias da seguinte entrada do serviço DAS_Binary_EventStore:

```
<service name="DAS_Binary_EventStore" plugins=""
strategyid="sentinel_client" subscriptiongroup="dasbin" />
```

4 Dê um nome exclusivo para cada uma das cópias das entradas dos serviços DAS_Binary e DAS_Binary_EventStore. Por exemplo, os nomes de serviço podem ser DAS_Binary1, DAS_Binary_EventStore1, DAS_Binary2 e DAS_Binary_EventStore2.

5 Localize a seção do arquivo `configuration.xml` que define as entradas de processos (veja o exemplo abaixo). Faça uma cópia da entrada do processo DAS_Binary para cada instância do DAS_Binary que deseja executar. Por exemplo, para executar dois processos DAS_Binary, faça duas cópias da entrada do processo DAS_Binary. Para cada entrada do processo DAS_Binary, modifique as seções da entrada conforme descrito a seguir:

- **DAS_Binary Dsrv_name:** Mude para que corresponda aos nomes do serviço DAS_Binary definidos na etapa 4, como DAS_Binary2.
- **Nome do serviço de comunicação do DAS_Binary:** Insira o texto a seguir no atributo image da entrada do processo, no local mostrado em negrito no exemplo de entrada de processo abaixo. Para cada entrada do processo DAS_Binary, substitua a parte DAS_Binary do texto abaixo pelo nome de serviço associado, como DAS_Binary2.

  ```
  -Desecurity.communication.service=DAS_Binary
  ```
- **Nome do arquivo `das_binary.xml` :** Use nomes exclusivos, como `das_binary_2.xml`. Esses nomes serão usados em uma etapa posterior.
- **Nome do arquivo das_binary_log_prop:** Use nomes exclusivos, como `das_binary_log_2.prop`. Esses nomes serão usados em uma etapa posterior.
- **Nome do diretório das_binary.cache:** Use nomes exclusivos, como `das_binary2.cache`. Cada instância do DAS_Binary deverá usar um diretório `das_binary.cache` diferente.
- **Nome do processo DAS_Binary:** Mude o valor do atributo name da entrada do processo para que corresponda aos nomes do serviço DAS_Binary definidos na etapa 4, como DAS_Binary2.

O xml a seguir é um exemplo de entrada de processo que aplica as instruções fornecidas acima:

```
process component="DAS" depends="UNIX Communication Server,Windows
Communication Server" image="&quot;$(ESEC_JAVA_HOME)/java&quot; -
server -Dsrv_name=DAS_Binary -Xmx160m -Xms64m -XX:+UseParallelGC -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=../log/
DAS_Binary.hprof -Xss136k -Xrs -
Desecurity.communication.service=DAS_Binary -Duser.language=en  -
Djava.net.preferIPv4Stack=true -Dfile.encoding=UTF8 -
Desecurity.cache.directory=../data/das_binary.cache -
Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml -
Djava.util.logging.config.file=../config/das_binary_log.prop -
Dcom.esecurity.configurationfile=../config/configuration.xml -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../config/krb5.conf -jar ../lib/
ccsbase.jar ..//config//das_binary.xml" min_instances="1"
name="DAS_Binary" post_startup_delay="20" type="container"
working_directory="$(ESEC_HOME)/data"/>
```

6 Grave o arquivo `configuration.xml`.

7 Localize o arquivo `das_binary.xml` no diretório $ESEC_HOME/config (%ESEC_HOME%\config no Windows).

8 Crie uma cópia do arquivo `das_binary.xml` para cada instância do DAS_Binary que deseja executar. Por exemplo, para executar duas instâncias do DAS_Binary, crie duas cópias de `das_binary.xml`.

9 Renomeie os arquivos `das_binary.xml` copiados para que seus nomes correspondam aos nomes selecionados na etapa 5.

10 Faça as seguintes mudanças em todos os arquivos `das_binary.xml`:

- Faça uma cópia do componente DispatchManager inteiro e mude o ID do novo componente de DispatchManager para EventStoreDispatchManager. Depois que você fizer essa mudança, um dos componentes terá o ID DispatchManager e o outro, o ID EventStoreDispatchManager.
- Atualize o valor da propriedade `esecurity.communication.service` do componente DispatchManager com o nome exclusivo apropriado do DAS_Binary, como DAS_Binary2.
- Atualize o valor da propriedade `esecurity.communication.service` do componente EventStoreDispatchManager com o nome exclusivo apropriado do DAS_Binary_EventStore, como DAS_Binary_EventStore2.
- Remova a propriedade `handler:esecurity.event.create` do componente DispatchManager.
- Remova todas as propriedades cujo nome comece com "handler:*", exceto `handler:esecurity.event.create`, do componente EventStoreDispatchManager. A sub-rotina `handler:esecurity.event.create` deverá ser a única sub-rotina definida no componente EventStoreDispatchManager.
- Adicione o seguinte elemento XML ao componente EventStoreService.

```
<obj-component-ref>
   <name>DispatchManager</name>
   <ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

11 Grave os arquivos `das_binary.xml`.

12 Localize o arquivo `das_binary_log.prop` no diretório $ESEC_HOME/config (%ESEC_HOME%\config no Windows).

13 Crie uma cópia do arquivo `das_binary_log.prop` para cada instância do DAS_Binary que deseja executar. Por exemplo, para executar duas instâncias do DAS_Binary, crie duas cópias de `das_binary_log.prop`.

14 Renomeie os arquivos `das_binary_log.prop` para que seus nomes correspondam aos nomes selecionados na etapa 5.

15 Reinicie o serviço do Sentinel para ativar as mudanças.

No UNIX:

```
$ESEC_HOME/bin/sentinel.sh restart
```

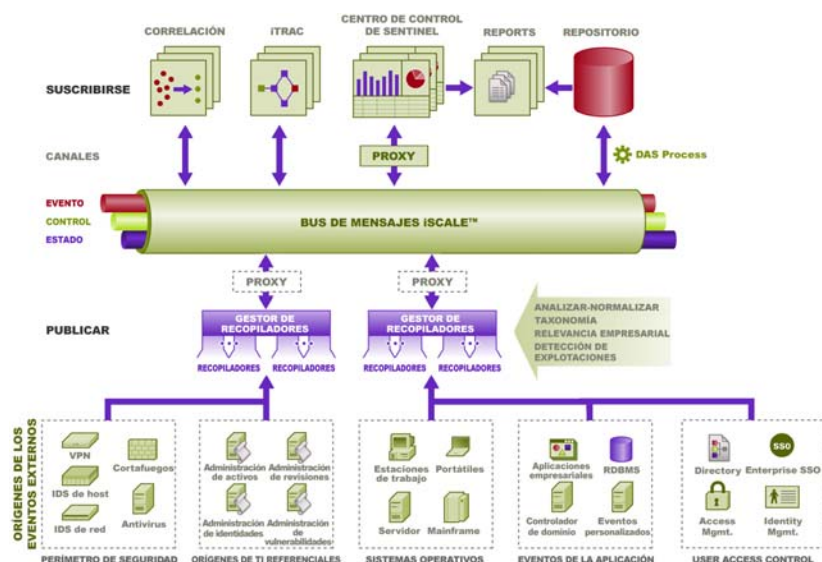
No Windows:

```
Restart the "Sentinel" service using the Windows Service Manager.
```

Camada de comunicação (iSCALE)

7

A camada de comunicação (iSCALE) que conecta todos os componentes da arquitetura é uma conexão criptografada baseada em TCP/IP criada em um backbone JMS (Java Messaging Service). No Sentinel 6, um proxy SSL opcional foi adicionado para proteger o Gerenciador de Coletor e os componentes do Sentinel Control Center, caso eles estejam instalados fora do firewall.

***Figura 7-1** Arquitetura do Sentinel*

Você poderá escolher dentre duas opções de comunicação ao instalar o Gerenciador de Coletor:

- **Conectar diretamente ao barramento de mensagem (padrão):** Essa é a opção mais simples e rápida. Ela exige que o Gerenciador de Coletor conheça a chave criptográfica compartilhada do barramento de mensagem. No entanto, isso poderá ser um risco de segurança se o Gerenciador de Coletor estiver sendo executado em uma máquina que esteja exposta a ameaças de segurança (por exemplo, uma máquina no DMZ). Essa opção criptografará a comunicação usando criptografia AES de 128 bits com base nos dados contidos em um arquivo chamado `.keystore`.
- **Conectar ao barramento de mensagem por meio de proxy:** Essa opção adiciona uma camada de segurança extra, configurando o Gerenciador de Coletor para se conectar por meio de um servidor proxy SSL. Nesse caso, a criptografia e a autenticação baseada em certificação serão usadas para que o `.keystore` não precise ser armazenado na máquina do Gerenciador de Coletor. Essa é uma boa opção quando o Gerenciador de Coletor está instalado em um ambiente menos seguro.

Você poderá selecionar uma dessas duas opções ao instalar o Gerenciador de Coletor. Por padrão, o Sentinel Control Center usa o proxy.

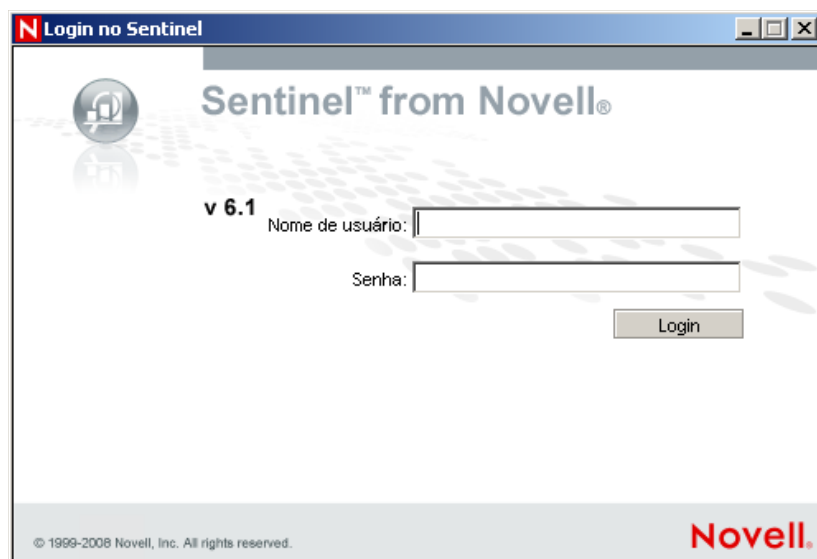
7.1 Proxy SSL e comunicação direta

Os componentes do Sentinel que podem usar o proxy SSL são o Sentinel Control Center e o Gerenciador de Coletor.

7.1.1 Sentinel Control Center

Por padrão, o Sentinel Control Center usa o proxy SSL. O Sentinel Control Center se conecta ao SSL por meio da porta `proxied_client`. Essa porta é configurada para usar apenas a autenticação de certificado SSL do servidor. A autenticação do cliente usa o nome de usuário e a senha do usuário do Sentinel Control Center.

Para efetuar login no Sentinel Control Center pela primeira vez:

1 Vá para Start (Iniciar) > Programs (Programas) > Sentinel e selecione Sentinel Control Center. A janela de login do Sentinel é exibida.

2 Forneça suas credenciais de usuário para efetuar login no Sentinel Control Center.
   - Nome de usuário e senha, se estiver usando a autenticação do SQL Server OU
   - Domínio\nome de usuário e senha, se estiver usando a autenticação do Windows

3 Clique em Login.

4 Será exibida uma mensagem de aviso, conforme mostrado na figura abaixo, para a primeira tentativa de login.

5. Se você selecionar Aceitar, essa mensagem será exibida sempre que você tentar abrir o Sentinel em seu sistema. Para evitar isso, selecione Aceitar permanentemente.

Para iniciar o Sentinel Control Center no Linux e no Solaris:

1. Como Usuário do Administrador do Sentinel (esecadm), mude o diretório para:
   `$ESEC_HOME/bin`
2. Execute o seguinte comando:
   `control_center.sh`
3. Forneça seu nome de usuário e sua senha e clique em OK.
4. Será exibida uma janela de certificação, clique em Aceitar.

Os usuários do Sentinel Control Center precisarão repetir o procedimento acima para aceitar um novo certificado quando:

- O servidor de comunicação do Sentinel for reinstalado
- O servidor de comunicação do Sentinel for movido para um novo servidor

7.1.2 Gerenciador de Coletor

O Gerenciador de Coletor pode ser instalado no modo proxy (por meio do proxy SSL) ou no modo direto (por meio de conexão direta com o barramento de mensagem).

- Para Gerenciadores de Coletor que possam ser comprometidos mais facilmente (por exemplo, uma máquina no DMZ), o proxy SSL é o método de comunicação mais seguro.
- Para Gerenciadores de Coletor em ambientes mais seguros, Gerenciadores de Coletor que precisam obter um alto throughput de eventos ou Gerenciadores de Coletor instalados na mesma máquina que o DAS (Serviço de Acesso a Dados), é recomendável usar a comunicação direta com o barramento de mensagem.

O Gerenciador de Coletor se conecta ao SSL por meio do `proxied_trusted_client`. Para habilitar o Gerenciador de Coletor para ser reiniciado sem intervenção humana depois de uma reinicialização, essa porta é configurada para usar a autenticação de certificação SSL do servidor e

do cliente. Um relacionamento de confiança é estabelecido entre o proxy e o Gerenciador de Coletor (troca de certificados), com conexões futuras usando os certificados para autenticação. Esse relacionamento de confiança é configurado automaticamente durante a instalação.

O relacionamento de confiança precisará ser redefinido para cada Gerenciador de Coletor que use o proxy SSL quando:

- O servidor de comunicação do Sentinel for reinstalado
- O servidor de comunicação do Sentinel for movido para um novo servidor

Você também poderá usar esse procedimento para mudar o modo do Gerenciador de Coletor de modo direto para modo de proxy.

Para redefinir o relacionamento de confiança de um Gerenciador de Coletor:

1. Efetue login no servidor do Gerenciador de Coletor como Administrador do Sentinel (o padrão é esecadm).
2. Abra o arquivo `configuration.xml` em $ESEC_HOME/config ou %ESEC_HOME%\config usando um editor de texto.
3. Modifique os serviços "Collector_Manager", "agentmanager_events" e "Sentinel" do `configuration.xml` para que usem o ID de estratégia "proxied_trusted_client". Veja a seguir uma amostra do arquivo de exemplo:

```
<service name="Collector_Manager" plugins=""
strategyid="proxied_trusted_client"/>
<service name="agentmanager_events" plugins=""
strategyid="proxied_trusted_client"/>
<service name="Sentinel" plugins=""
strategyid="proxied_trusted_client"/>
```

4. Grave o arquivo e saia.
5. Execute `%ESEC_HOME%\bin\register_trusted_client.bat` (ou o arquivo `.sh` se estiver no UNIX). Você verá uma saída semelhante a esta:

```
E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
Please review the following server certificate:
Type: X.509
Issued To: foo.bar.net
Issued By: foo.bar.net
Fingerprint (MD5): A8:DF:BA:B2:F3:21:C9:27:28:48:13:B3:FE:F8:B4:AD
Would you like to accept this certificate? [Y/N] (defaults to N): Y
Please enter a Sentinel username and password that has permissions
to register a trusted client.
Username: esecadm
Password:*********
*Writing to keystore file: E:\Program
Files\Novell\Sentinel6\config\.proxyClientKeystore
```

6. Reinicie o Serviço do Sentinel no servidor que hospeda o Gerenciador de Coletor.
7. Repita essas etapas em todos os Gerenciadores de Coletor usando a comunicação proxy.

7.2 Mudando a chave criptográfica de comunicação

A instalação do Sentinel permite que o administrador gere uma nova chave criptográfica aleatória (armazenada no arquivo `.keystore`) ou importe um arquivo `.keystore` existente. Em ambas as abordagens, para que a comunicação funcione corretamente, o arquivo `.keystore` deverá ser o mesmo em todas as máquinas em que o componente Sentinel Server estiver instalado.

Observação: O arquivo `.keystore` não será necessário na máquina do banco de dados se o banco de dados for o único componente do Sentinel instalado nessa máquina. Esse arquivo também não será necessário nas máquinas em que apenas o Sentinel Control Center, o Construtor de Coletor, o Gerenciador de Dados do Sentinel ou o Gerenciador de Coletor (usando proxy) estiver instalado.

Você poderá mudar a chave criptográfica após a instalação usando o utilitário `keymgr`. Esse utilitário gera um arquivo contendo uma chave criptográfica produzida aleatoriamente. Esse arquivo deve ser copiado em todas as máquinas com um componente do Sentinel Server instalado.

Para mudar a chave criptográfica para Comunicação Direta:

1. No UNIX, efetue login como Usuário do Administrador do Sentinel (o padrão é esecadm). No Windows, efetue login como um usuário com direitos administrativos.
2. Consulte:

   Para UNIX:

   ```
   $ESEC_HOME/lib
   ```

   Para Windows:

   ```
   %ESEC_HOME%\lib
   ```
3. Execute o seguinte comando:

   No UNIX:

   ```
   keymgr.sh --keyalgo AES --keysize 128 --keystore <output filename,
   usually .keystore>
   ```

   No Windows:

   ```
   keymgr.bat --keyalgo AES --keysize 128 --keystore <output filename,
   usually .keystore>
   ```
4. Copie `.keystore` em todas as máquinas com um componente do Sentinel Server instalado (a menos que esteja usando a comunicação proxy). O arquivo deve ser copiado em:

   Para UNIX:

   ```
   $ESEC_HOME/config
   ```

   Para Windows:

   ```
   %ESEC_HOME%\config
   ```

Observação: Se estiver usando o Advisor no modo Download Direto, você deverá atualizar a senha armazenada nos arquivos de configuração do Advisor. Essa senha é criptografada com as informações contidas no arquivo `.keystore` e deve ser recriada com o novo valor do `.keystore`. Para atualizar a senha, siga as instruções fornecidas no Capítulo 4, “Configuração do Advisor” na página 63.

7.3 Aumentado a força da chave AES

O Sentinel usa criptografia AES para comunicação pelo Sonic e senhas criptográficas armazenadas nos arquivos config e enviadas pelo Sonic. Por padrão, o Sentinel usa o algoritmo de criptografia AES de 128 bits devido a determinadas restrições de importação. Se essas restrições de importação não se aplicarem a você, configure o Sentinel para usar um algoritmo AES de 256 bits, que é mais avançado.

Observação: É altamente recomendável que você consulte a seção "Understanding the Export/ Import Issues" ("Compreendendo os problemas de exportação/importação") do arquivo `Readme.txt` do Java antes de habilitar a criptografia de 256 bits.

Para configurar a criptografia AES de 256 bits:

1 Faça download de políticas de criptografia ilimitada do Sun em http://java.sun.com/javase/downloads/index_jdk5.jsp (http://java.sun.com/javase/downloads/index_jdk5.jsp). Na seção Other Downloads (Outros Downloads), faça download do "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0".

2 Aplique o arquivo de política mencionado acima a todos os JREs que executarem processos que se conectem diretamente ao Sonic (DAS, Mecanismo de Correlação, Servidor de Comunicação, Gerenciador de Coletor, caso seja usado no modo Direto para o Sonic). Para saber como aplicar arquivos de política, consulte o `Readme.txt` disponível na política transferida por download.

3 Use o utilitário keymgr para gerar um arquivo `.keystore` de `AES` de 256 bits seguindo as instruções fornecidas na seção Seção 7.2, "Mudando a chave criptográfica de comunicação" na página 95.

4 Copie esse arquivo `.keystore` em todas as máquinas mencionadas na etapa 2 e coloque-o no diretório $ESEC_HOME/config ou %ESEC_HOME%\config.

Observação: Se estiver usando o Advisor no modo Download Direto, você deverá atualizar a senha armazenada nos arquivos de configuração do Advisor. Essa senha é criptografada com as informações contidas no arquivo `.keystore` e deve ser recriada com o novo valor do `.keystore`. Para obter mais informações sobre como atualizar uma senha, consulte a seção "Gerenciamento de certificação do DAS_Proxy" no *Guia de Referência*.

Crystal Reports para Windows

8

O Crystal Reports Server™ (da Business Objects) é a ferramenta de geração de relatórios usada com o Sentinel. Esta seção aborda a instalação e a configuração do Crystal Reports Server para Sentinel. Para obter mais informações sobre plataformas suportadas para o Crystal Reports Server em ambientes Sentinel, consulte o Capítulo 2, "Requisitos do sistema" na página 21.

No Windows, o Sentinel foi testado com o Crystal Reports Server XI R2 SP3. Para obter mais informações sobre Crystal Reports Server XI Release 2 Service Packs, consulte https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads) e procure a plataforma e a versão corretas.

Esta seção aborda a execução do Crystal Reports Server no Windows. Para obter mais informações sobre a execução do Crystal Reports Server no Linux/Solaris, consulte o .

Para Instalar o Crystal Reports Server:

1. Instale o Microsoft IIS e o ASP.NET
2. Instale o Microsoft SQL (dependendo da configuração: autenticação do Windows ou autenticação do SQL Server)
3. Somente para usuários chineses (tradicional e simples) e japoneses: instale fontes asiáticas (por exemplo, Arial Unicode MS) para ver os relatórios nesses idiomas
4. Instale o Crystal Reports Server
   - Configurando o Open Database Connectivity (ODBC) para Autenticação do SQL

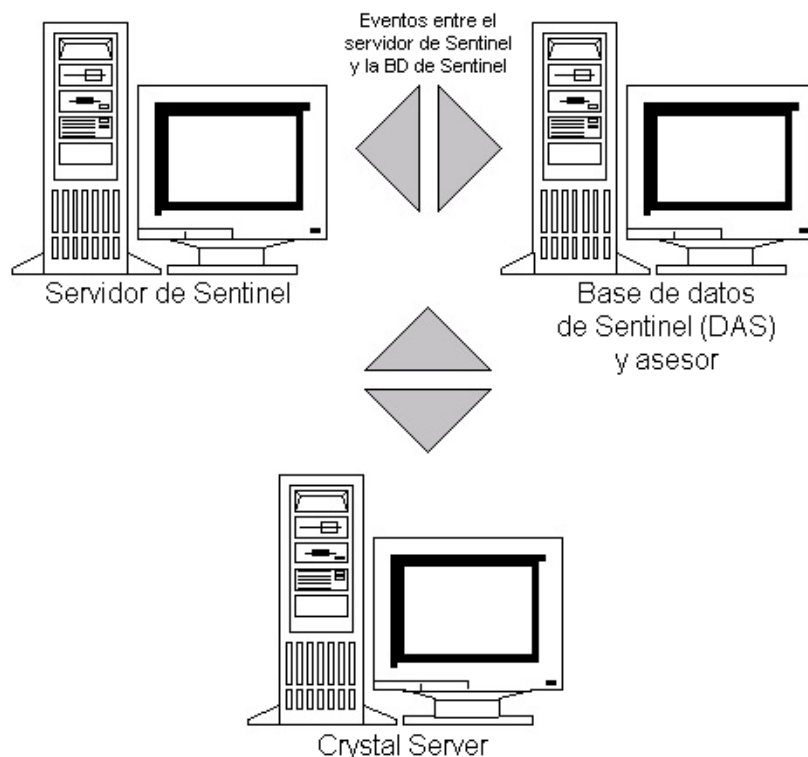
     ou

   - Instalando e configurando o software cliente do Oracle 9i
5. Configure o `inetmgr`
6. Aplique os patches do Crystal Reports
7. Publique (importe) o Crystal Reports
8. Defina uma Conta de Usuário Nomeado
9. Teste a conectividade com o servidor Web

10 Aumente o limite de registro de atualização de relatório do Crystal Reports Server (recomendado)

11 Configure o Sentinel Control Center para integrar-se ao Crystal Reports Server

---

Observação: Você deve instalar os componentes na ordem fornecida acima.

8.1 Visão geral

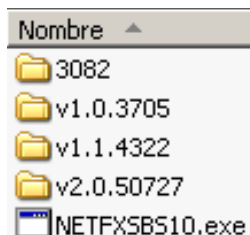
O Crystal Reports Server requer um banco de dados para armazenar informações sobre o sistema e seus usuários. Esse banco de dados é conhecido como o banco de dados do Servidor de Gerenciamento Central (CMS). O CMS é um servidor que armazena informações sobre o sistema do Crystal Reports Server. Outros componentes do Crystal Reports Server podem acessar essas informações de acordo com a necessidade.

Para instalar o Crystal no Windows, é necessário configurar o banco de dados CMS em um banco de dados local do Microsoft SQL Server. Embora o instalador do Crystal Reports Server permita configurar o banco de dados CMS no banco de dados MSDE, essa configuração não foi testada e não é suportada no Sentinel.

8.2 Requisitos do sistema

Windows® 2003 Server com SP1 com uma partição formatada em NTFS com o IIS (Microsoft Internet Information Server) e o ASP.NET instalados. O Sentinel não suporta o Crystal XI R2 no Windows® 2000 Server.

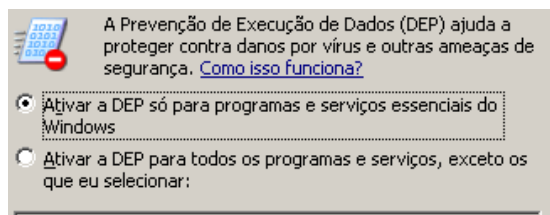
.NET Framework 1.1 ou 2.0 (instalado por padrão no Windows 2003). Para determinar que versão do .NET Framework está instalada em sua máquina, vá para %SystemRoot%\Microsoft.NET\Framework. A pasta com o maior valor numérico não deve ser maior do que v.1.1.xxxx. Por exemplo:

Figura 8-1 *Versão do .NET Framework*

Para obter mais informações sobre plataformas suportadas para o Crystal Reports Server em ambientes Sentinel, consulte Capítulo 2, “Requisitos do sistema” na página 21.

8.3 Requisitos de configuração

1. Verifique se a conta usada para instalar o Crystal Reports Server é um administrador local.
2. Configure a DEP (Prevenção de Execução de Dados) para ser executada apenas em programas e serviços essenciais do Windows. Isso é particularmente útil para evitar o erro “Error 1920. Service Crystal Report Cache Server on Windows 2003” ("Erro 1920. Servidor de Cache do Serviço Crystal Report no Windows 2003”).

   Para acessar a DEP, vá para Controle Panel (Painel de Controle) > System (Sistema) > guia Advanced (Avançado) > Performance Settings (Configurações de Desempenho) > Data Execution Prevention (Prevenção de Execução de Dados).

   Selecione Turn on DEP for essential Windows programs and services only (Ativar a DEP só para programas e serviços essenciais do Windows).

3. As instruções de instalação e configuração do Crystal Reports Server pressupõem que o servidor e o banco de dados do Sentinel já tenham sido instalados. Você precisa saber que modo de autenticação foi escolhido para o usuário do Sentinel Report. O usuário será chamado esecrpt, se você estiver utilizando a autenticação de banco de dados local. Se estiver utilizando a Autenticação do Windows, você poderá escolher o nome que desejar para o usuário. O modo de autenticação foi definido em uma tela semelhante à mostrada abaixo durante o processo de instalação do Sentinel.

Autenticación de Windows

Autenticación de SQL Server

Entrada a la sesión:

Observação: A senha de esecrpt poderá ser explicitamente definida caso o Windows seja usado.

4 A resolução de vídeo deve ser definida como 1024 x 768 ou mais.

5 Instale o Microsoft Internet Information Server (IIS) e o ASP.NET.

Observação: O Sentinel não suporta o uso do MSDE como banco de dados CMS do Crystal. Instale o Microsoft SQL Server 2005 antes de instalar o Crystal Reports Server XI R2.

8.3.1 Instalando o Microsoft Internet Information Server (IIS) e o ASP.NET

Para adicionar esses componentes do Windows, talvez seja necessário usar o CD de instalação do Windows 2003 Server.

Para instalar o IIS e o ASP.NET:

1 Vá para Control Panel (Painel de Controle) > Add/Remove Programs (Adicionar ou Remover Programas).

2 No painel vertical esquerdo, clique em Add/Remove Windows Components (Adicionar/ Remover Componentes do Windows).

3 Selecione Application Server (Servidor de Aplicativos).

4 Clique em Details (Detalhes).

5 Selecione ASP.NET e Internet Information Services (IIS).

6 Clique em OK.

7 Clique em Next (Avançar). Você poderá ser solicitado a usar o CD de instalação do Windows.

8 Clique em Finish (Concluir).

8.4 Problemas conhecidos

- **Instalando o Crystal Reports:** A Novell emite duas chaves do Crystal, uma para o Crystal Reports Server e a outra para o Crystal Reports Developer (para a modificação ou a criação de novos relatórios). Use a chave do Crystal Reports Server ao instalar o Crystal Reports Server.
- **Desinstalando o Crystal Reports:** Caso seja necessário desinstalar o Crystal Reports Server, há um procedimento manual de desinstalação disponível que limpa as chaves do registro. Isso é útil quando a instalação é corrompida. Visite o seguinte site da Business Objects na web para obter os procedimentos necessários para a desinstalação manual do Crystal Reports Server: http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

Observação: Esse URL estava correto no momento da publicação deste documento.

8.5 Usando o Crystal Reports

Para obter mais informações sobre como usar o Crystal Reports Server para gerar relatórios do Sentinel, consulte a Documentação do Crystal Reports Server (http://support.businessobjects.com/documentation/product_guides/default.asp) e o *Guia do Usuário do Sentinel.*

8.6 Visão geral da instalação

8.6.1 Visão geral da instalação do Crystal com SQL Server 2005

Veja a seguir as etapas de alto nível que você deverá executar para instalar o Crystal Reports Server com um banco de dados do Sentinel no Microsoft SQL Server 2005 usando Autenticação do Windows ou Autenticação do SQL. As etapas são descritas em mais detalhes no restante desta seção.

1. Instale o Crystal Reports Server XI R2
    - Se tiver selecionado Autenticação do Windows para o usuário do Sentinel Report ao instalar o Sentinel, consulte a Seção 8.7.1, “Instalando o Crystal Reports Server para Microsoft SQL Server 2005 com Autenticação do Windows” na página 102.
    - Se tiver selecionado Autenticação do SQL para o usuário do Sentinel Report ao instalar o Sentinel, consulte a Seção 8.7.2, “Instalando o Crystal Reports Server para Microsoft SQL Server 2005 com Autenticação do SQL” na página 107.
2. Configure o ODBC (Open Database Connectivity)
3. Mapeie o Crystal Reports para ser usado com o Sentinel
4. Aplique os patches do Crystal Reports
5. Publique relatórios
6. Defina a Conta de Usuário Nomeado

7 Crie uma página do Crystal na web (Seção 8.9.5, “Configurando permissões de relatórios” na página 120)
8 Configure o Sentinel para o Crystal Reports Server

Observação: Essas etapas deve ser executadas na ordem apresentada.

8.6.2 Visão geral da instalação do Crystal com Oracle

Veja a seguir as etapas de alto nível que você deverá executar para instalar o Crystal Reports Server com um banco de dados do Sentinel no Oracle. As etapas são descritas em mais detalhes no restante desta seção.

Para instalar adequadamente o Crystal Reports, execute o procedimento a seguir na ordem apresentada.

1. Instale o Oracle Client e configure o driver nativo do Oracle
2. Somente para usuários chineses (tradicional e simples) e japoneses: instale fontes asiáticas (por exemplo, Arial Unicode MS) para ver os relatórios nesses idiomas.
3. Instale o Crystal Reports Server XI R2. Para obter mais informações, consulte a Seção 8.7.3, “Instalando o Crystal Reports Server para Oracle” na página 112.
4. Mapeie o Crystal Reports para ser usado com o Sentinel
5. Importe gabaritos do Crystal Reports
6. Crie uma página do Crystal na web (Seção 8.9.5, “Configurando permissões de relatórios” na página 120)
7. Configure o Sentinel para o Crystal Reports Server

Observação: Essas etapas deve ser executadas na ordem apresentada.

8.7 Instalação

Esta seção descreve como instalar o Crystal Reports Server para:

- Seção 8.7.1, “Instalando o Crystal Reports Server para Microsoft SQL Server 2005 com Autenticação do Windows” na página 102
- Seção 8.7.2, “Instalando o Crystal Reports Server para Microsoft SQL Server 2005 com Autenticação do SQL” na página 107
- Seção 8.7.3, “Instalando o Crystal Reports Server para Oracle” na página 112

8.7.1 Instalando o Crystal Reports Server para Microsoft SQL Server 2005 com Autenticação do Windows

Para instalar o Crystal Reports Server com Autenticação do Windows:

1. Instale o Microsoft SQL Server 2005 no modo misto.
2. Inicie o Microsoft SQL Server Management Studio.
3. No painel de navegação, expanda Databases (Bancos de Dados).

Realce e clique o botão direito do mouse em Database (Banco de Dados) e selecione New Database (Novo Banco de Dados) para criar o banco de dados CMS do Crystal.

4 No campo Database name (Nome do banco de dados), digite BOE115 e clique em OK.

5 Saia do Microsoft SQL Server Management Studio.

6 Insira o CD do Crystal Reports XI R2 Server na unidade de CD-ROM.

7 Se a opção Autoplay (Reprodução Automática) estiver desabilitada, execute o `setup.exe`.

8 Selecione o idioma de configuração do Crystal Reports.

9 Na janela Select Client or Server Installation (Selecionar Instalação de Cliente ou Servidor), selecione Perform Server Installation (Executar Instalação de Servidor).

10 Forneça a chave de licença do Crystal (obtida no Novell Customer Center (https://secure-www.novell.com/center/regadmin)).

11 Especifique uma pasta de destino.

12 Para o tipo de instalação, selecione Use an existing database server (Usar o servidor de banco de dados existente).

13 No painel do banco de dados CMS, clique em Browse (Procurar).

14 Clique na guia Machine Data Source (Fonte de Dados da Máquina). Clique em New (Novo).

15 Selecione System Data Source (Fonte de Dados do Sistema).

Clique em Next (Avançar).

16 Role para baixo, selecione SQL Server e clique em Next (Avançar).

17 Uma nova fonte é exibida. Clique em Finish (Concluir).

Origen de datos de sistema
Controlador: SQL Server

18 Na janela New Data Source (Nova Fonte de Dados) do SQL Server, especifique:

- O nome da fonte de dados (por exemplo, BOE_XI)
- A descrição (opcional)
- Para o servidor, clique na seta para baixo e selecione (local)

Clique em Next (Avançar).

19 Se ainda não tiver feito isso, selecione With Windows NT (Com Windows NT) e clique em Next (Avançar).

Observação: A opção Login ID (ID de Logon), que aparece esmaecida e indisponível, é seu nome de login do Windows.

20 Marque a caixa de seleção Change the default database to (Mudar o banco de dados padrão para). Mude o banco de dados padrão para BOE115. Clique em Next (Avançar).

21 Na janela Create a New Data Source to SQL Server (Criar Nova Fonte de Dados para SQL Server), clique em Finish (Concluir).

22 Clique em Test Data Source (Testar Fonte de Dados) e teste a fonte de dados. Depois de testar a fonte de dados, clique em OK.

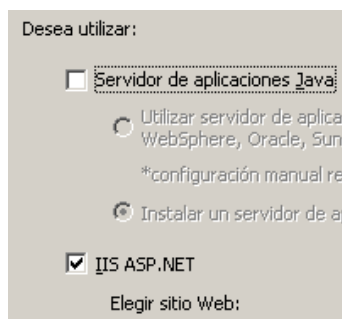
23 Na janela Select Data Source (Selecionar Fonte de Dados), realce BOE115 e continue clicando em OK até que SQL Server Login (Logon do SQL Server) seja exibido. Verifique se Use Trusted Connection (Usar Conexão Confiável) está selecionado. Clique em OK.

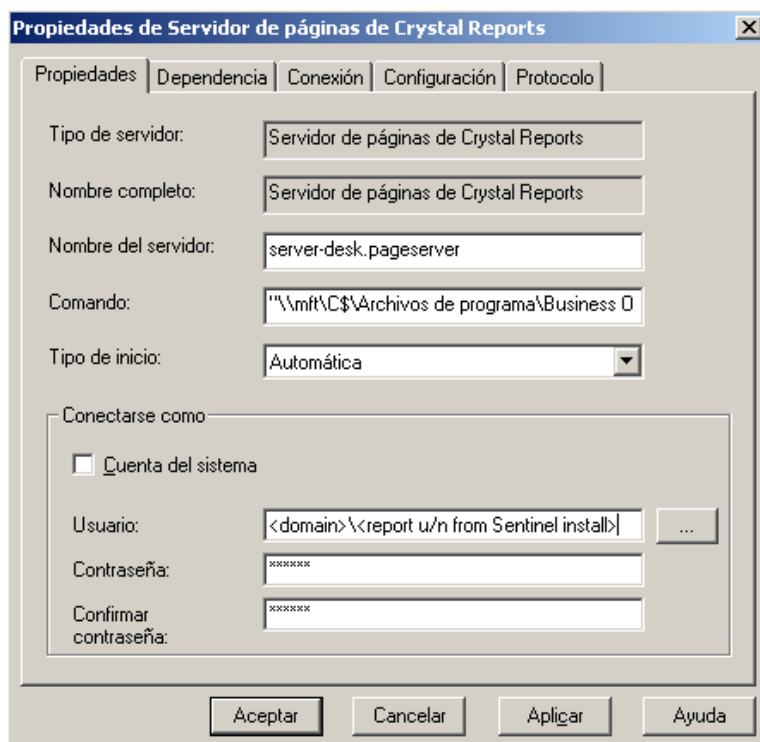
Observação: A opção Login ID (ID de Logon), que aparece esmaecida e indisponível, é seu nome de login do Windows.

---

24 Na janela Web Component Adapter Type (Tipo de Adaptador de Componente Web), selecione IIS ASP.NET.

Observação: Se você não tiver instalado o IIS e o ASP.NET pelo caminho Control Panel (Painel de Controle) > Add Remove Programs (Adicionar ou Remover Programas) > Add/Remove Windows Components (Adicionar/Remover Componentes do Windows), a opção IIS ASP.NET ficará esmaecida (indisponível).

---

25 Após a instalação, será preciso mudar a conta de login para o Crystal Reports Page Server e o Crystal Reports Job Server para a conta de domínio do Usuário do Sentinel Report.

- Clique em Start (Iniciar) > Programs (Programas) > BusinessObjects > Crystal Reports Server > Central Configuration Manager.
- Clique o botão direito do mouse em Crystal Reports Page Server e selecione Stop (Parar).
- Clique novamente o botão direito em Crystal Reports Page Server e selecione Properties (Propriedades).
- Desmarque Log On As System Account (Efetuar Logon como Conta do Sistema) e especifique o nome de usuário e a senha de domínio do Usuário do Sentinel Report usados durante a instalação do Sentinel. Clique em OK.

26 Realce Crystal Reports Page Server e clique o botão direito do mouse para iniciá-lo.

Configurando o Open Database Connectivity (ODBC) para Autenticação do Windows

Esse procedimento configura um nome de fonte de dados ODBC para permitir que o Crystal Reports Server se conecte ao banco de dados do Sentinel no Windows e no SQL Server usando a autenticação do Windows. Essas etapas devem ser executadas na máquina em que o Crystal Reports Server se encontra.

Para configurar uma fonte de dados ODBC para Autenticação do Windows:

1. Vá para o Control Panel (Painel de Controle) > Administrative Tools (Ferramentas Administrativas) > Data Sources (ODBC) (Fontes de Dados (ODBC)) no Windows.
2. Clique na guia System DSN (DSN de Sistema) e no botão Add (Adicionar).
3. Selecione SQL Server. Clique em Finish (Concluir).
4. É exibida uma janela solicitando informações de configuração do driver:
   - Em Data Source name (Nome da Fonte de Dados), especifique esecuritydb
   - No campo Description (Descrição) (opcional), forneça uma descrição
   - No campo Server (Servidor), forneça o nome de host ou o endereço IP do Sentinel Server

5 Clique em Next (Avançar).

Na janela seguinte, selecione Windows Authentication (Autenticação do Windows).

Observação: A opção Login ID (ID de Logon), que aparece esmaecida e indisponível, é seu nome de login do Windows.

---

6 Na janela seguinte, selecione:

- Change the Sentinel database (Mudar o banco de dados do Sentinel) (o nome padrão é ESEC)
- Leave all the default settings (Manter todas as configurações padrão)

Clique em Next (Avançar).

7 Clique em Finish (Concluir).

8 Clique em Test Data Source (Testar Fonte de Dados). Uma conexão é estabelecida. Clique em OK até sair.

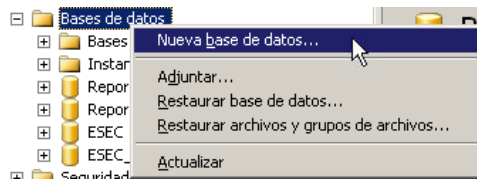
8.7.2 Instalando o Crystal Reports Server para Microsoft SQL Server 2005 com Autenticação do SQL

Para instalar o Crystal Reports Server com Autenticação do SQL:

1 Instale o Microsoft SQL Server 2005.

2 Inicie o Microsoft SQL Server Management Studio.

3 No painel de navegação, expanda Databases (Bancos de Dados).

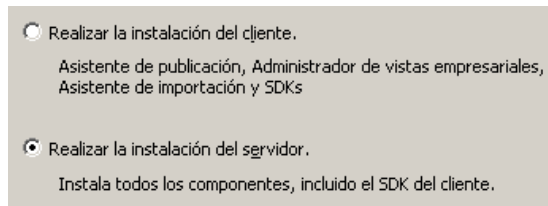
Realce e clique o botão direito do mouse em Database (Banco de Dados) e selecione New Database (Novo Banco de Dados) para criar o banco de dados CMS do Crystal.

4 No campo Database name (Nome do banco de dados), digite BOE115 e clique em OK.

5 Saia do Microsoft SQL Server Management Studio.

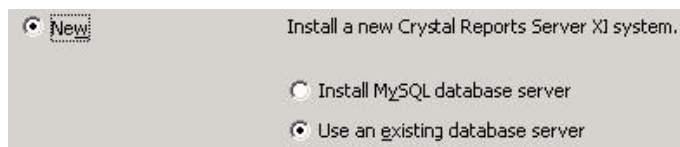
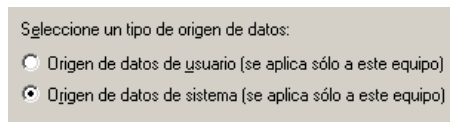
6 Insira o CD do Crystal Reports Server XI R2 na unidade de CD-ROM.

7 Se a opção Autoplay (Reprodução Automática) estiver desabilitada, execute o `setup.exe`.

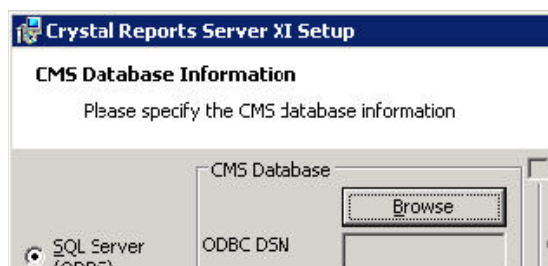
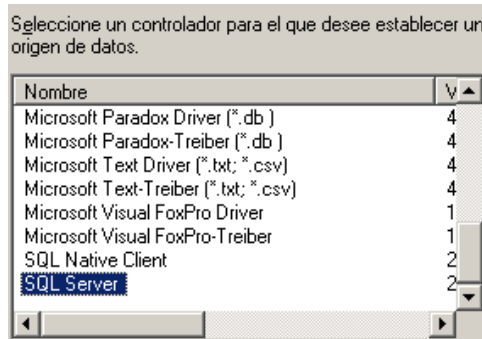
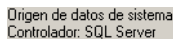
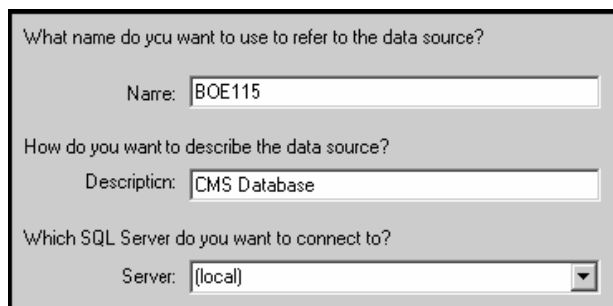
8 Selecione o idioma de configuração do Crystal Reports.

9 Na janela Select Client or Server Installation (Selecionar Instalação de Cliente ou Servidor), selecione Perform Server Installation (Executar Instalação de Servidor).

10 Forneça a chave de licença do Crystal (obtida no Novell Customer Center (https://secure-www.novell.com/center/regadmin)).

11 Especifique uma pasta de destino.

12 Para o tipo de instalação, selecione Use an existing database server (Usar o servidor de banco de dados existente).

Observação: O Crystal Reports Server e o Microsoft SQL Server devem residir na mesma máquina.

---

13 No painel do banco de dados CMS, clique em Browse (Procurar).

14 Clique na guia Machine Data Source (Fonte de Dados da Máquina) e clique em New (Novo). Selecione System Data Source (Fonte de Dados do Sistema).

Clique em Next (Avançar).

Role para baixo, selecione SQL Server e clique em Next (Avançar).

Uma nova fonte é exibida. Clique em Finish (Concluir).

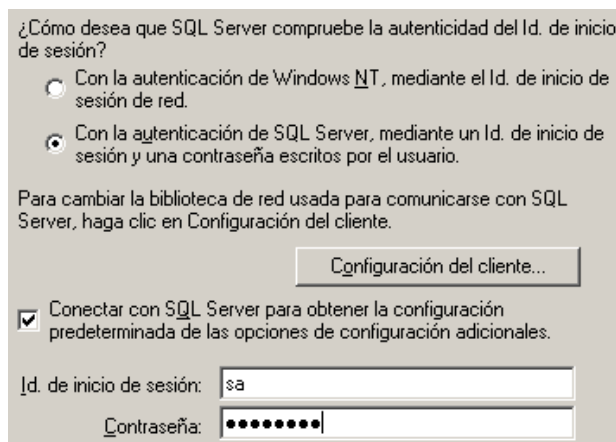
Origen de datos de sistema
Controlador: SQL Server

15 Clique o botão direito do mouse em Databases (Bancos de Dados) e selecione Create New Database (BOE115) (Criar Novo Banco de Dados (BOE115)).

16 Na janela New Data Source (Nova Fonte de Dados) do SQL Server, especifique:

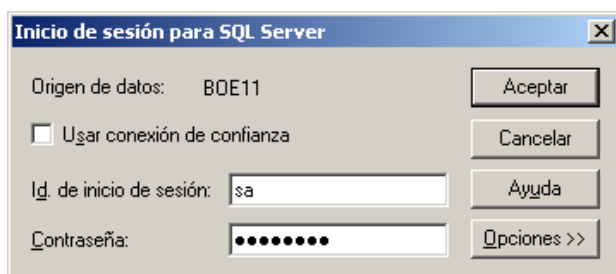
- O nome da fonte de dados (por exemplo, BOE115)
- A descrição (opcional)
- Para o servidor, clique na seta para baixo e selecione (local)

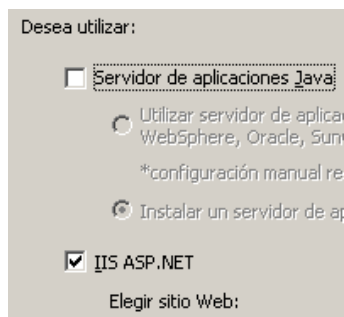
Clique em Next (Avançar).

17 Selecione With SQL Server authentication (Com autenticação do SQL Server) e insira sa e a senha de sa. Clique em Next (Avançar).

Marque a caixa de seleção Change the default database to (Mudar o banco de dados padrão para). Mude o banco de dados padrão para BOE115. Clique em Next (Avançar).

18 Na janela Create a New Data Source to SQL Server (Criar Nova Fonte de Dados para SQL Server), clique em Finish (Concluir).

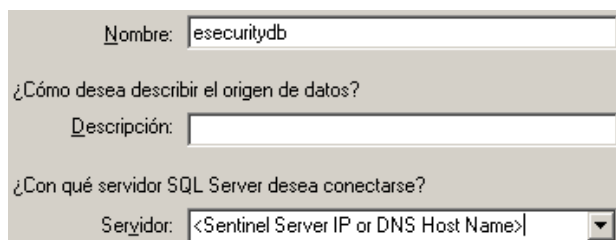
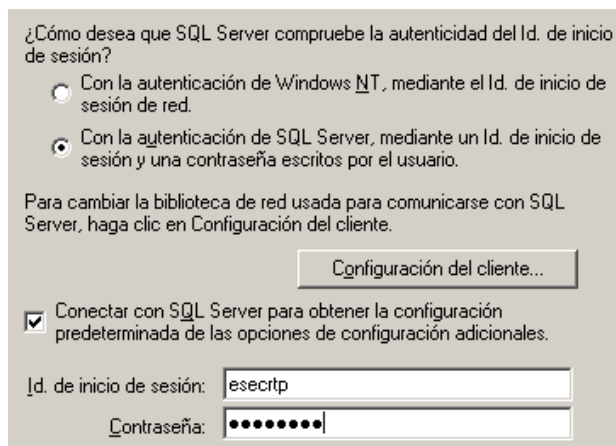
19 Clique em Test Data Source (Testar Fonte de Dados). Clique em OK.

Na janela Select Data Source (Selecionar Fonte de Dados), realce BOE115 e continue clicando em OK até que SQL Server Login (Logon do SQL Server) seja exibido. Assegure-se de que Use Trusted Connection (Usar Conexão Confiável) NÃO esteja selecionado. Clique em OK. Clique em Next (Avançar).

20 Na janela Web Component Adapter Type (Tipo de Adaptador de Componente Web), selecione IIS ASP.NET.

Observação: Se você não tiver instalado o IIS e o ASP.NET pelo caminho Control Panel (Painel de Controle) > Add Remove Programs (Adicionar ou Remover Programas) > Add/Remove Windows Components (Adicionar/Remover Componentes do Windows), a opção IIS ASP.NET ficará esmaecida (indisponível).

Configurando o Open Database Connectivity (ODBC) para Autenticação do SQL

Esse procedimento configura um nome de fonte de dados ODBC para permitir que o Crystal Reports Server se conecte ao banco de dados do Sentinel no Windows e no SQL Server usando a autenticação do SQL. Essas etapas devem ser executadas na máquina em que o Crystal Reports Server se encontra.

Para configurar uma fonte de dados ODBC para Windows:

1. Vá para o Control Panel (Painel de Controle) > Administrative Tools (Ferramentas Administrativas) > Data Sources (ODBC) (Fontes de Dados (ODBC)) no Windows).
2. Clique na guia System DSN (DSN de Sistema) e no botão Add (Adicionar).
3. Selecione SQL Server. Clique em Finish (Concluir).
4. É exibida uma janela solicitando informações de configuração do driver:
   - Em Data Source name (Nome da Fonte de Dados), especifique esecuritydb
   - No campo Description (Descrição) (opcional), forneça uma descrição
   - No campo Server (Servidor), especifique o nome de host ou o endereço IP do Sentinel Server

   Clique em Next (Avançar).
5. Na janela seguinte, selecione SQL Authentication (Autenticação do SQL). Forneça esecrpt e a senha como ID de logon. Clique em Next (Avançar).

6 Na janela seguinte, selecione:
- Change the Sentinel database (Mudar o banco de dados do Sentinel) (o nome padrão é ESEC)
- Leave all the default settings (Manter todas as configurações padrão)

Clique em Next (Avançar) e em Finish (Concluir).

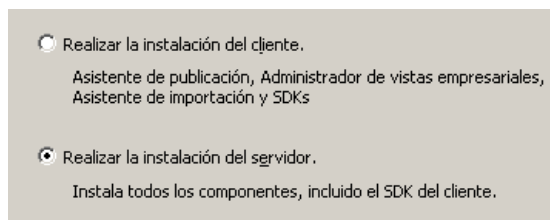
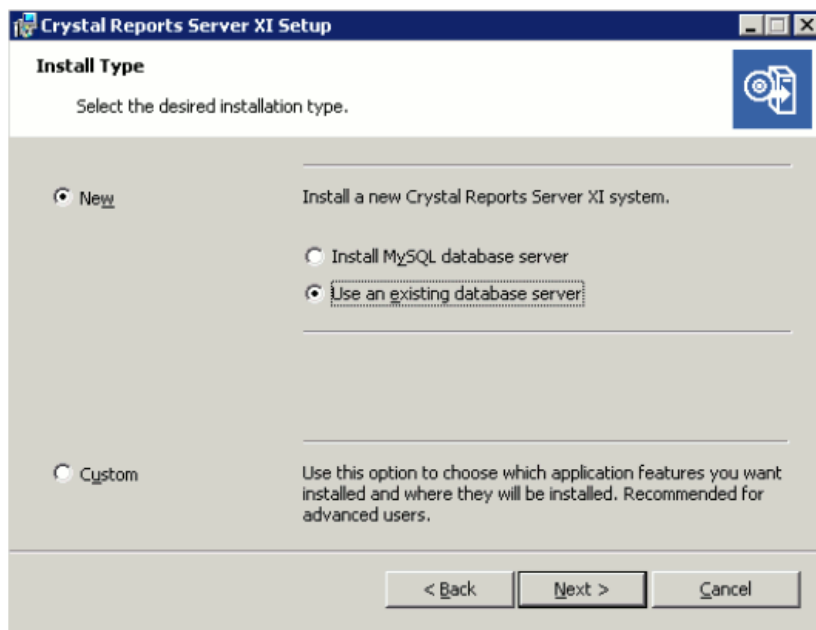
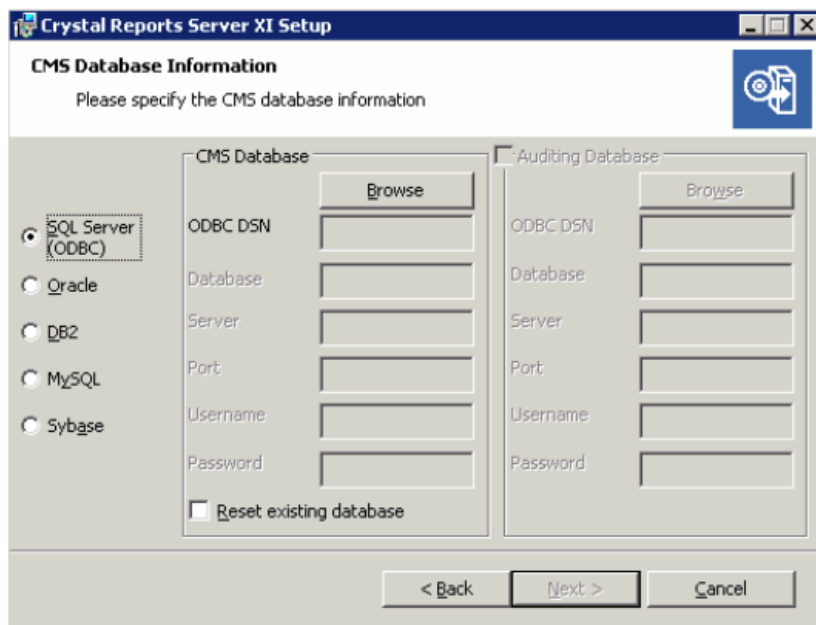
7 Clique em Test Data Source (Testar Fonte de Dados). Após o teste, clique em OK. Clique em OK até sair.

8.7.3 Instalando o Crystal Reports Server para Oracle

Para instalar o Crystal Reports XI R2 Server para Oracle:

1 Insira o CD do Crystal Reports XI R2 Server na unidade de CD-ROM.

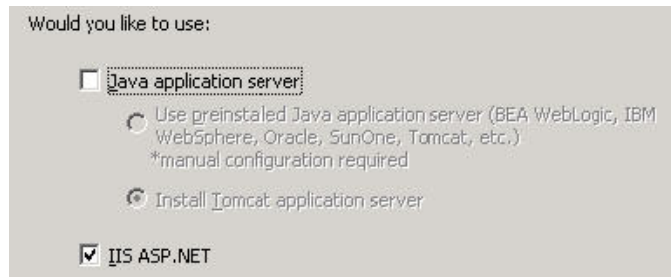
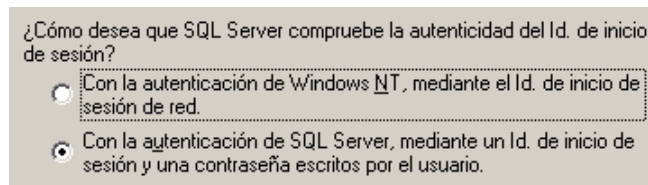
2 Selecione o idioma de configuração do Crystal Reports.

3 Na janela Select Client or Server Installation (Selecionar Instalação de Cliente ou Servidor), selecione Perform Server Installation (Executar Instalação de Servidor).

4 Selecione Use an existing database server (Usar o servidor de banco de dados existente).

A janela CMS Database Information (Informações do Banco de Dados CMS) é exibida:

Selecione o tipo SQL Server (ODBC) e clique em Browse (Procurar) para escolher um DSN. Depois de selecionar um DSN, você será solicitado a fornecer um nome de usuário e uma senha. Forneça as informações solicitadas e clique em Next (Avançar).

Observação: O Crystal Reports Server e o Microsoft SQL Server 2005 devem residir na mesma máquina.

---

5 Selecione IIS ASP.NET.

Observação: Se você não tiver instalado o IIS e o ASP.NET pelo caminho Control Panel (Painel de Controle) > Add Remove Programs (Adicionar ou Remover Programas) > Add/Remove Windows Components (Adicionar/Remover Componentes do Windows), a opção IIS ASP.NET ficará esmaecida (indisponível). A instalação do IIS e do ASP.NET é um pré-requisito para esta instalação.

6 Você será solicitado a especificar o Authentication Mode (Modo de Autenticação). Selecione a autenticação do SQL Server.

O Crystal Reports Server suporta acesso direto a um banco de dados do Sentinel no Oracle. Esse tipo de acesso é fornecido pelo arquivo de conversão crdb_oracle.dll. Esse arquivo se comunica com o driver do banco de dados Oracle, que funciona diretamente com bancos de dados Oracle e clientes, recuperando os dados necessários para seu relatório.

Observação: Para que o Crystal Reports Server use bancos de dados Oracle, o software cliente Oracle deve ser instalado no sistema e o local do cliente Oracle deve estar na variável de ambiente PATH.

Instalando e configurando o software cliente Oracle

Ao instalar o cliente Oracle:

- Aceite o local de instalação padrão
- Não – para Perform Typical Configuration (Realizar Configuração Típica)
- Não – para Directory Service (Serviço de Diretório)
- Selecione Local
- TNS Service Name (Nome do Serviço TNS): ESEC
- User (Usuário) (opcional): esecrpt

Após a instalação, crie uma configuração de nome de serviço de rede local.

O procedimento a seguir é destinado ao driver nativo do Oracle 9, mas é semelhante ao procedimento do Oracle 10.

Para criar a configuração do nome de serviço de rede (configurando o driver nativo do Oracle 9):

1. Selecione Oracle-OraHome92 > Configuration and Migration Tools (Ferramentas de Configuração e Migração) > Net Manager.
2. No painel de navegação, expanda Local e realce Service Naming (Nome de Serviço).
3. Clique no sinal de mais à esquerda para adicionar um nome de serviço.
4. Na janela Service Name (Nome do Serviço), forneça um nome de serviço de rede.
   - Digite ESECURITYDB.

   Clique em Next (Avançar).
5. Na janela Select Protocols (Selecionar Protocolos), selecione o padrão:
   - TCP/IP (Protocolo da Internet)

   Clique em Next (Avançar).
6. Em Host Name (Nome do Host) e Port Number (Número da Porta):
   - Forneça o nome de host ou o endereço IP da máquina em que reside o banco de dados do Sentinel
   - Selecione a porta do Oracle (padrão 1521 durante a instalação)

   Clique em Next (Avançar).
7. Para identificar o banco de dados ou o serviço do Sentinel:
   - Selecione Oracle8i ou posterior e forneça o nome do serviço (o nome da instância do Oracle).
   - Para o tipo de conexão, selecione Database Default (Banco de Dados Padrão).

   Clique em Next (Avançar).
8. Na janela Test (Teste), clique em Test (Testar). Clique em Next (Avançar). Poderá ocorrer falha, pois o teste usa um ID de banco de dados e uma senha.
9. Se o teste falhar, execute este procedimento:
   - Na janela Connection Test (Teste de Conexão), clique em Change Login (Mudar Login).
   - Forneça o ID do Sentinel no Oracle (use esecrpt) e a senha. Clique em Test (Testar).

   Se o teste falhar:
   - Use o comando ping no Sentinel Server
   - Verifique se o nome de host do Sentinel Server está no arquivo de hosts do Crystal Reports Server. Esse arquivo se encontra em %SystemRoot%\system32\drivers\etc\.
10. Clique em Close (Fechar) e, em seguida, clique em Finish (Concluir).

8.8 Configurando todas as autenticações e configurações

Os procedimentos a seguir são necessários para que o Crystal Reports Server funcione com o Sentinel Control Center.

8.8.1 Configurando inetmgr

Para configurar inetmgr:

1. Copie o arquivo `web.config` de:

   `C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content`

   para c:\Inetpub\wwwroot.
2. Inicie o Internet Service Manager (Gerenciador de Serviços de Internet) clicando em Start (Iniciar) > Run (Executar). Digite inetmgr e clique em OK.
3. Expand (local computer) (Expandir (computador local)) > Web Sites (Sites) > Default Web Site (Site Padrão) > businessobjects.
4. Em businessobjects, clique o botão direito do mouse > properties (propriedades).
5. Na guia Virtual Directory (Diretório Virtual), clique em Configuration (Configuração).
6. Você deverá ter os mapeamentos a seguir. Caso não os tenha, adicione-os. Se você for adicionar um mapeamento, não clique nos nós businessobjects ou crystalreportsviewer11.

Extensão	Executável
`.csp`	`C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll`
`.cwr`	`C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll`
`.cri`	`C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll`
`.wis`	`...\BusinessObjects Enterprise 11.5`

   Clique em OK para fechar a janela.
7. Reinicie o IIS. Para isso, vá para Expand (local computer) (Expandir (computador local)) > Web Sites (Sites) > Default Web Site (Site Padrão), realce Default Web Site (Site Padrão) e clique o botão direito do mouse em Stop (Parar).
8. Vá para Expand (local computer) (Expandir (computador local)) > Web Sites (Sites) > Default Web Site (Site Padrão), realce Default Web Site (Site Padrão) e clique o botão direito do mouse em Start (Iniciar).

8.9 Publicando gabaritos do Crystal Reports

Muitos gabaritos de relatório são criados pela Novell para serem usados nas guias Análise e Advisor do Sentinel Control Center. Para fazer download do conjunto de relatórios mais recente, visite as páginas de conteúdo do Sentinel 6 na Web no seguinte URL:

http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html)

O conjunto básico de relatórios do Sentinel são distribuídos no Sentinel Core Solution Pack.

Você pode adicionar relatórios ao sistema de quatro maneiras:

- Faça download de um Solution Pack na guia Solution Packs e use o Gerenciador de Soluções para instalar um ou mais controles que incluam relatórios.
- Faça download de um Collector Pack na guia Coletores e use o Gerenciador de Soluções para instalar um ou mais controles que incluam relatórios.
- Adicione um ou mais gabaritos de relatório (arquivos .rpt) usando o Assistente de Publicação do Crystal.
- Adicione um ou mais gabaritos de relatório (arquivos .rpt) usando o Crystal Reports Central Management Console.

Importante: Para executar os 10 relatórios principais, habilite a agregação e ative o EventFileRedirectService no `DAS_Binary.xml`. Na instalação padrão do Sentinel, essa configuração já está definida. Para obter informações sobre como habilitar a agregação, consulte a seção “Configuração de dados de relatório” de “Admin” no *Guia do Usuário do Sentinel*.

8.9.1 Publicando gabaritos de relatório com o Gerenciador de Soluções

Se você configurar corretamente o servidor web e o Crystal Reports Server usando as instruções de instalação descritas neste capítulo, os relatórios incluídos em um Solution Pack ou em um Collector Pack poderão ser publicados diretamente no Crystal Reports Server por meio do Gerenciador de Soluções. Para obter mais informações, consulte a “Solution Packs” no *Guia do Usuário do Sentinel*.

8.9.2 Publicando Gabaritos de Relatórios - Assistente de Publicação do Crystal Reports

Agora, os relatórios do Sentinel serão distribuídos por meio de Solution Packs, mas esse método poderá ser usado para publicar gabaritos de relatório provenientes de uma origem que não seja um Solution Pack.

Para publicar os gabaritos do Crystal Report:

Observação: Se desejar publicar os Gabaritos de Relatórios novamente, apague os Gabaritos de Relatórios importados anteriormente.

---

1. Clique em Start (Iniciar) > Programs (Programas) > BusinessObjects > Crystal Reports Server > Assistente de Publicação.

   Clique em Avançar.
2. Efetue login. Em Sistema, forneça o nome de host da máquina em que o Crystal está instalado, e em Autenticação, especifique Enterprise. O Nome de Usuário pode ser Administrador. Por questões de segurança, é altamente recomendável que você crie um novo usuário, diferente de Administrador. Forneça sua senha e clique em Avançar.

   Observação: Relatórios publicados com o nome de usuário Administrador podem ser acessados por todos os usuários.

   ---

3 Clique em Adicionar Pasta. [Opcional] Selecione Incluir Subpastas.

4 Navegue para o local onde estão os gabaritos de relatório. Clique em OK. Clique em Avançar.

5 Na janela Especificar Local, clique em Nova Pasta (canto superior direito) e crie uma pasta chamada SentinelReports (caso ela ainda não exista). Clique em Avançar.

6 Selecione:

- Duplicar hierarquia de pasta.

  Clique na seta para baixo e selecione <não incluir nenhum>.

  Clique em Avançar.

7 Na janela Confirmar Localização, clique em Avançar.

8 Na janela Especificar Categorias, forneça o nome da categoria (como sentinel), realce o nome e clique no botão +.

Observação: Somente o primeiro relatório será exibido na categoria depois que você clicar em Avançar.

Clique em Avançar.

9 Na janela Especificar Programação, clique em Permitir que usuários atualizem o objeto (essa deve ser a opção padrão). Clique em Avançar.

10. Na janela Especificar Atualização do Repositório, clique em Habilitar Tudo para habilitar a atualização do repositório. Clique em Avançar.
11. Na janela Especificar Manutenção dos Dados Gravados, clique em Habilitar Tudo para manter os dados gravados quando publicar relatórios. Clique em Avançar.
12. Na janela Mudar Valores Padrão, clique em Publicar relatórios sem modificar propriedades (essa deve ser a opção padrão). Clique em Avançar.
13. Clique em Avançar para adicionar seus objetos.
14. Uma lista de publicações será exibida; clique em Concluir.

Quando forem publicados no Crystal Reports Server, os gabaritos do Sentinel para Crystal Reports deverão residir no diretório do SentinelReports; caso contrário, eles não serão exibidos no Sentinel Control Center.

8.9.3 Publicando gabaritos de relatório – Central Management Console

Agora, os relatórios do Sentinel serão distribuídos por meio de Solution Packs, mas esse método poderá ser usado para publicar gabaritos de relatório provenientes de uma origem que não seja um Solution Pack.

Para importar gabaritos do Crystal Report:

1. Abra um browser da web e forneça o seguinte URL:
   `http://<hostname_or_IP_of_web_server>/businessobjects/enterprise115/WebTools/adminlaunch`
2. Clique em Central Management Console
3. Efetue login no Crystal Reports Server.
4. No painel Organize (Organizar), clique em Folders (Pastas).
5. No canto superior direito, clique em New Folder (Nova Pasta).
6. Crie a pasta SentinelReports (caso ela ainda não exista). Clique em OK.

   Observação: É necessário que o nome da pasta seja SentinelReports.

7. Clique em SentinelReports.
8. Clique na guia Subpastas e crie subpastas se desejar. Se estiver adicionando os relatórios básicos do Sentinel manualmente, crie as seguintes subpastas:
   - Advisor_Vulnerability
   - Dashboards
   - Incident Management
   - Internal Events
   - Security Events
   - Top 10
9. Clique em Home > Objects (Objetos) > New Object (Novo Objeto).
10. À esquerda da página, realce Report (Relatório).

11. Clique em Browse (Procurar) para procurar os gabaritos de relatório a serem adicionados. Escolha uma pasta e selecione um relatório.
12. Realce SentinelReports e clique em Show Subfolders (Mostrar Subpastas).
13. Selecione a pasta apropriada para o relatório e clique em Show Subfolders (Mostrar Subpastas).
14. Clique em Submit (Submeter).
15. Para adicionar os relatórios restantes, repita as etapas 9 até 17 até que todos os relatórios tenham sido adicionados.

8.9.4 Definindo uma conta de usuário nomeado

A chave de licença fornecida com o Crystal Reports Server é uma chave de Conta de Usuário Nomeado. A conta Guest foi mudada de Concurrent User (Usuário Simultâneo) para Named User (Usuário Nomeado).

Para definir a conta Guest como Named User (Usuário Nomeado):

1. Clique em Start (Iniciar) > Programs (Programas) > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad.
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.
4. O nome de usuário deverá ser Administrator. Forneça sua senha (por padrão, esse campo está em branco). Clique em Log On (Efetuar Login). No painel Organize (Organizar), clique em Users (Usuários).
5. Clique em Guest.
6. Mude o tipo de conexão de Concurrent User (Usuário Simultâneo) para Named User (Usuário Nomeado).

   Importante: Para gerar relatórios ilimitados, use a conta Named User License (Licença de Usuário Nomeado).

7. Clique em Update (Atualizar).
8. Efetue logout e feche a janela ou vá para a seção Configurando o .NET Administration Launchpad.

8.9.5 Configurando permissões de relatórios

Esse procedimento discute como usar o .NET Administration Launchpad para configurar as permissões que permitirão que você veja e modifique relatórios sob demanda.

Para configurar permissões de relatórios:

1. Se ainda não tiver feito isso, inicie o .NET Administration Launchpad (clique em Start (Iniciar) > Programs (Programas) > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad).

Observação: Ao iniciar o .NET Administration Launchpad, se receber a mensagem de erro "HTTP 404 - File or Directory not found" ("HTTP 404 - Arquivo ou diretório não encontrado"), consulte http://support.microsoft.com/kb/315122 (http://support.microsoft.com/kb/315122) para obter a resolução.

2 Clique em Central Management Console.

   O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.

3 O nome de usuário deverá ser Administrator. Forneça sua senha (por padrão, esse campo está em branco). Clique em Log On (Efetuar Login). No painel Organize (Organizar), clique em Folders (Pastas).

4 Clique em SentinelReports.

5 Selecione tudo.

6 Clique na guia Rights (Direitos).

7 Em Everyone (Todos), no menu suspenso à direita de Access Level (Nível de Acesso), selecione View on Demand (Ver por Demanda).

8 Clique em Update (Atualizar).

9 Efetue logout e feche a janela.

Testando a conexão do servidor web com o Banco de Dados do Sentinel

Para testar a conexão do servidor web com o banco de dados:

1. Se ainda não tiver feito isso, inicie o .NET Administration Launchpad (Start (Iniciar) > Programs (Programas) > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad).
2. Clique em Central Management Console.
3. O Nome de Usuário deverá ser Administrador. Forneça sua senha (por padrão, esse campo está em branco). Clique em Efetuar Login.
4. Navegue para Pastas > SentinelReports > Internal Events.
5. Selecione Detalhes de Exibição de Coluna.
6. Clique em Visualizar.
7. Dependendo do sistema, efetue login como esecrpt ou como o Usuário do Sentinel Report.
8. No menu suspenso do campo de classificação, selecione Tag.
9. Clique em OK. Um relatório é exibido.

Testando a conectividade com o servidor web

Para testar a conectividade com o servidor web:

1. Vá para outra máquina situada na mesma rede que o servidor web.
2. Especifique

```
http://<DNS name or IP address of your web server>/businessobjects/
enterprise115/WebTools/adminlaunch/default.aspx
```

A página do Crystal BusinessObjects na Web será exibida.

8.9.6 Desabilitando os 10 Principais Relatórios do Sentinel

Por padrão, os 10 Principais Relatórios do Sentinel são habilitados. Se você acha que não usará esses relatórios, reduza o armazenamento do banco de dados e o uso da CPU desabilitando os 10 Principais Relatórios do Sentinel:

- Desativar agregação
- Desabilitar EventFileRedirectService

Para desativar agregação:

1. Inicie o Sentinel Control Center.
2. Efetue login.
3. Clique na guia Admin e abra a opção Relatando Dados.
4. Desabilite os seguintes resumos:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Clique em Ativo na coluna Status até que mude para Inativo.

Nombre del res...	Hora	Atributos	Origen	Estado
EventDestSum...	1 hora	CUST_ID,RS ...	TransformedEv...	Activo
EventSevDestT...	1 hora	CUST_ID,DE ...	TransformedEv...	Inactivo
EventSevDestE...	1 hora	CUST_ID,DE ...	TransformedEv...	Inactivo
EventSevDestP...	1 hora	SEV,DEST_F ...	TransformedEv...	Inactivo
EventSevSumm...	1 hora	CUST_ID,SE ...	TransformedEv...	Activo
EventSrcSumm...	1 hora	CUST_ID,RS ...	TransformedEv...	Activo

Para desabilitar EventFileRedirectService:

1. Na máquina DAS, usando o editor de texto, abra:

   Para UNIX:

   ```
   $ESEC_HOME/config/das_binary.xml
   ```

   Para Windows:

   ```
   %ESEC_HOME%\config\das_binary.xml
   ```

2. Para o EventFileRedirectService, mude o status para off (desativado).

   ```
   <property name="status">off</property>
   ```

3. Reinicie o componente DAS, executando este procedimento:

   No Windows:

   ```
   Use Service Manager to stop and then start the “sentinel” service
   ```

8.9.7 Configurando o Sentinel Control Center para integrar-se ao Crystal Reports Server

O Sentinel Control Center pode ser configurado para se integrar ao Crystal Reports Server. Isso permitirá que você veja o Crystal Reports a partir do Sentinel Control Center.

Para habilitar a integração do Sentinel Control Center com o Crystal Reports Server, siga as instruções abaixo.

Observação: Essa configuração só deverá ser executada depois que o Crystal Reports Server for instalado e que os relatórios do Crystal forem publicados nele.

Para configurar o Sentinel para se integrar ao Crystal Reports Server:

1 Efetue login no Sentinel Control Center como um usuário com privilégios na guia Admin.

2 Na guia Admin, selecione Configuração do Crystal Report.

3 No campo URL de Análise, forneça o seguinte:

```
http://<hostname_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Observação: <nome_de_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou pelo nome de host do Crystal Reports Server.

Observação: O URL acima não funcionará corretamente se o APS (programador automatizado de processos) estiver definido como o endereço IP. Ele deve ser o nome de host do Crystal Reports Server.

4 Clique em Atualizar ao lado do campo URL de Análise.

5 Se o Advisor estiver instalado, forneça o seguinte no campo URL do Advisor:

```
http://<hostname_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Observação: <nome_de_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou pelo nome de host do Crystal Reports Server.

Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele deve ser o nome de host do Crystal Reports Server.

6 Clique em Atualizar ao lado do campo URL do Advisor.

7 Clique em Gravar.

8 Efetue logout e, em seguida, efetue login novamente no Sentinel Control Center. As árvores do Crystal Report nas guias Análise e Advisor (se o Advisor estiver instalado) agora aparecerão na janela Navegador.

8.10 Configurações de alto desempenho para o Crystal

8.10.1 Aumentando o limite de registro de atualização do relatório do Crystal Reports Server

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para configurar o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server. Para fazer isso, use o Central Configuration Manager ou a página do Crystal na web.

Para reconfigurar o Crystal Page Server usando o Central Configuration Manager:

1. Clique em Start (Iniciar) > All Programs (Todos os Programas) > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
2. Clique o botão direito do mouse em Crystal Reports Page Server e selecione Parar.
3. Clique o botão direito em Crystal Reports Page Server e selecione Propriedades.
4. Na guia Propriedades do campo Comando, no final da linha de comando, adicione:
   ```
   maxDBResultRecords <value greater than 20000 or 0 to disable the
   default limit>
   ```
5. Reinicie o Crystal Page Server.

Para reconfigurar o Crystal Page Server usando o Central Management Console:

1. Clique em Start (Iniciar) > All Programs (Todos os Programas) > Businessobjects 11 > Crystal Reports Server > .Net Administration Launchpad. Como alternativa, você poder abrir um browser da web e fornecer o seguinte URL:

   http://<Nome DNS ou endereço IP do servidor web>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.
4. Forneça seu nome de usuário e sua senha e clique em Log On (Efetuar Login). Clique em Servers (Servidores).
5. Clique em <nome do servidor>.pageserver.
6. Em Database Records to Read When Previewing Or Refreshing a report (Registros do Banco de Dados para Ler quando Visualizar ou Atualizar um Relatório), selecione Unlimited records (Registros ilimitados). Clique em Apply (Aplicar).
7. Você será solicitado a reiniciar o servidor de página. Clique em OK.

Talvez seja preciso fornecer um nome de login e uma senha para acessar o gerenciador de serviço do sistema operacional.

8.10.2 Relatórios usando serviço de agregação

Para melhorar o desempenho, os 10 principais relatórios incluídos no Solution Pack do Sentinel Core consultam tabelas de resumo em vez de tabelas de eventos. As tabelas de resumo contêm contagens feitas ao longo do tempo para combinações de campos nos dados de eventos. Isso fornece um conjunto de dados muito menor para determinados tipos de consulta e resulta em consultas muito mais rápidas e tempos de execução de relatórios reduzidos.

O serviço de agregação é responsável pelo preenchimento das tabelas de resumo com resumos de todos os eventos da tabela de eventos. O serviço de agregação só gerará dados resumidos para resumos que ativos. Os resumos a seguir são exigidos pelos 10 principais relatórios e são habilitados por padrão:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Os resumos podem ser ativados ou desativados na janela de configuração de Relatando Dados na guia Admin do Sentinel Control Center.

O serviço de agregação também depende do componente `EventFileRedirectService` do DAS Binary para alimentá-lo com os dados de eventos que serão resumidos. Portanto, esse componente deve ser habilitado para que o serviço de agregação seja executado adequadamente. Para habilitar ou desabilitar esse componente, modifique o atributo "status" do componente `EventFileRedirectService` do `das_binary.xml` para "on" (ativado) ou "off" (desativado). Por padrão, o status do componente está "on" (ativado).

Observação: Para obter informações sobre EventFileRedirectService e os três resumos de agregação, consulte "Configuração de dados de relatório" em Admin, no *Guia do Usuário do Sentinel*.

Observação: Os relatórios que consultam uma grande faixa de datas podem demorar para serem executados. Você pode programá-los em vez de executá-los interativamente. Para obter informações sobre como programar o Crystal Reports, consulte a documentação do Crystal BusinessObjects Enterprise™ 11 (http://support.businessobjects.com/documentation/product_guides/default.asp).

8.10.3 Desenvolvimento do relatório

Você pode usar o Crystal Reports Developer para criar ou modificar relatórios. Para desenvolver relatórios personalizados, é recomendável o seguinte:

- Se os relatórios puderem utilizar tabelas agregadas predefinidas, selecione a tabela agregada resultante do processamento da menor quantidade de dados.
- Tente distribuir a maior parte do processamento de dados para o mecanismo de banco de dados.
- Para reduzir o overhead de processamento no Crystal Server, minimize a quantidade de dados a ser recuperada para o Crystal Server.
- Sempre grave relatórios nas telas do banco de dados fornecidas pela Novell, e não nas tabelas básicas.

Crystal Reports para Linux

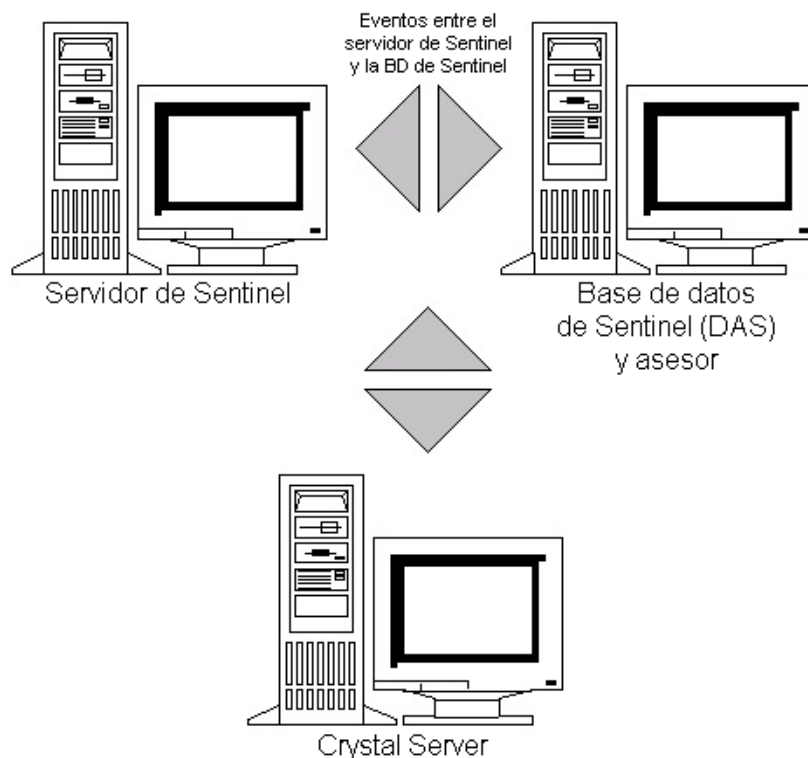
O Crystal Reports Server™ (da Business Objects) é a ferramenta de geração de relatórios usada com o Sentinel. Esta seção aborda a instalação e a configuração do Crystal Reports Server para Sentinel. Para obter mais informações sobre plataformas suportadas para o Crystal Reports Server em ambientes Sentinel, consulte o Capítulo 2, “Requisitos do sistema” na página 21.

No Linux, o Sentinel foi testado com o Crystal Reports Server XI R2 SP2. Para obter mais informações sobre Crystal Reports Server XI Release 2 Service Packs ou para transferi-los por download, consulte https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads) e procure a plataforma e a versão corretas.

Esta seção aborda a execução do Crystal Reports Server no Linux. Para obter mais informações sobre a execução do Crystal Reports Server no Windows, consulte o Capítulo 8, “Crystal Reports para Windows” na página 97.

Importante: A instalação deve ser feita na ordem apresentada abaixo.

Para instalar o Crystal Reports Server:

1. Pré-instale e instale o Crystal Reports Server™ XI R2
2. Aplique os patches do Crystal Reports Server
3. Publique (importe) o Crystal Reports
4. Defina uma conta de “Usuário Nomeado”
5. Teste a conectividade com o servidor web
6. Habilite os 10 relatórios principais (opcional)
7. Aumente o limite de registro de atualização de relatório do Crystal Reports Server (recomendado)
8. Configure o Sentinel Control Center para integrar-se ao Crystal Reports Server

9.1 Visão geral

O Crystal Reports Server requer um banco de dados para armazenar informações sobre o sistema e seus usuários. Esse banco de dados é conhecido como o banco de dados do Servidor de Gerenciamento Central (CMS). O CMS é um servidor que armazena informações sobre o sistema do Crystal Reports Server. Outros componentes do Crystal Reports Server podem acessar essas informações de acordo com a necessidade.

9.2 Instalação

9.2.1 Pré-instalação do Crystal Reports Server™ XI R2

Para pré-instalar o Crystal Reports Server:

1 Se o Banco de Dados do Sentinel não estiver na mesma máquina que o Crystal Reports Server, você deverá instalar o software cliente Oracle na máquina do Crystal Reports Server. Esta etapa adicional não será necessária se o Banco de Dados do Sentinel estiver na mesma máquina que o Crystal Reports Server, pois, nesse caso, o software Oracle exigido já terá sido instalado durante a instalação do banco de dados Oracle.

2 Efetue login na máquina do Crystal Reports Server como usuário root.

3 Crie o grupo bobje:

```
groupadd bobje
```

4 Crie um usuário do Crystal (o diretório pessoal deste exemplo é /export/home/crystal, mas você poderá mudá-lo se necessário; a parte /export/home do caminho já deve existir).

```
useradd –g bobje –s /bin/bash –d /export/home/crystal –m crystal
```

5 Crie um diretório para o software Crystal:

```
mkdir –p /opt/crystal_xir2
```

6 Mude a propriedade do diretório do software Crystal (recursivamente) para crystal/bobje:

```
chown -R crystal:bobje /opt/crystal_xir2
```

7 Você deverá conceder permissões ao usuário crystal no diretório $ORACLE_HOME usando uma Lista de Controle de Acesso (ACL). Pressupondo que o usuário do Crystal seja “crystal” e que $ORACLE_HOME seja `/opt/oracle/product/10.2/db_1`, o comando de execução será:

```
setfacl -m u:crystal:rx -R  /opt/oracle/product/10.2/db_1
```

Para verificar se a ACL foi definida corretamente, execute o seguinte comando e procure “crystal” na saída:

```
getfacl  /opt/oracle/product/10.2/db_1
```

8 Mude para o usuário crystal:

```
su - crystal
```

9 A variável de ambiente ORACLE_HOME deve ser definida no ambiente do usuário crystal. Para fazer isso, modifique o script de login do usuário crystal para definir a variável de ambiente ORACLE_HOME como a base do software Oracle. Por exemplo, se o shell do usuário crystal for bash e o software Oracle estiver instalado no diretório `/opt/oracle/product/10.2/db_1`, abra o arquivo `~crystal/.bash_profile` (`.profile` no SLES) e adicione a seguinte linha ao final do arquivo:

```
export ORACLE_HOME=/opt/oracle/product/10.2/db_1
```

10 A variável LD_LIBRARY_PATH do ambiente do usuário crystal deve conter o caminho para as bibliotecas do software Oracle. Para fazer isso, modifique o login script do usuário crystal para definir a variável de ambiente LD_LIBRARY_PATH para incluir as bibliotecas do software Oracle. Por exemplo, se o shell do usuário crystal for bash, abra o arquivo `~crystal/.bash_profile` e adicione a seguinte linha ao final do arquivo (abaixo da variável de ambiente ORACLE_HOME definida):

```
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

11 A variável PATH do ambiente do usuário crystal deve conter o caminho para os executáveis do software Oracle. Para fazer isso, modifique o login script do usuário crystal para definir a variável de ambiente PATH para incluir os executáveis do software Oracle. Por exemplo, se o shell do usuário crystal for bash, abra o arquivo `~crystal/.bash_profile` e adicione a seguinte linha ao final do arquivo:

```
export PATH=$PATH:$ORACLE_HOME/bin
```

12 Adicione uma entrada ao arquivo `tnsnames.ora` do Oracle com o nome de serviço esecuritydb, que aponta para o Banco de Dados do Sentinel. Para fazer isso na máquina do Crystal Reports Server:

12a Efetue login como usuário do Oracle.

12b Mude os diretórios para $ORACLE_HOME/network/admin.

12c Faça backup do arquivo `tnsnames.ora`.

12d Abra o arquivo `tnsnames.ora` para edição.

12e Se o Banco de Dados do Sentinel estiver na máquina do Crystal Reports Server, já deverá haver uma entrada no arquivo `tnsnames.ora` para o Banco de Dados do Sentinel. Por exemplo, se o banco de dados do Sentinel se chamar ESEC, existirá uma entrada semelhante a esta:

```
ESEC =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

12f Se o Banco de Dados do Sentinel não estiver na máquina do Crystal Reports Server, abra o arquivo `tnsnames.ora` na máquina do Banco de Dados do Sentinel para localizar a entrada descrita acima.

12g Faça uma cópia de toda a entrada e cole-a no final do arquivo `tnsnames.ora` da máquina do Crystal Reports Server. A parte da entrada que corresponde ao Nome do Serviço deve ser renomeada como `esecuritydb`. Por exemplo, se a entrada acima for copiada e renomeada corretamente, ela terá a seguinte aparência:

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

12h Verifique se a parte da entrada que corresponde a HOST está correta (por exemplo, ela não deverá estar definida como localhost se o Crystal Reports Server e o Banco de Dados do Sentinel estiverem em máquinas diferentes).

12i Grave as mudanças feitas no arquivo `tnsnames.ora`.

12j Execute o seguinte comando para verificar se o Nome do Serviço `esecuritydb` está configurado corretamente:

```
tnsping esecuritydb
```

12k Após executar o comando, você receberá uma mensagem informando que a conexão está OK.

9.2.2 Instalando o Crystal Reports Server XIR2

O instalador do Crystal Reports Server consiste em dois arquivos `.iso`. Durante a instalação, você será solicitado a fornecer a localização do segundo disco.

Para instalar o Crystal Reports Server:

1. Efetue login como usuário crystal.
2. Mude os diretórios para disk1 do instalador do Crystal.
3. Execute:

```
./install.sh
```

4 Selecione o idioma: English (Inglês).
5 Selecione New Installation (Nova Instalação).
6 Leia e aceite o Contrato de Licença.
7 Forneça o código da chave do produto.
8 Forneça o diretório de instalação:
   ```
   /opt/crystal_xir2
   ```
9 Selecione: User install (Instalação do usuário).
10 Selecione: New Install (Nova Instalação).
11 Selecione: Install MySQL unless you plan to install the Crystal CMS database into an existing database (Instalar MySQL a menos que você planeje instalar o banco de dados CMS do Crystal em um banco de dados existente).
12 Especifique informações de configuração para MySQL:
   12a Use a porta padrão 3306
   12b Senha Admin
13 Especifique mais informações de configuração para MySQL:
   13a Nome de banco de dados padrão: BOE115
   13b ID do usuário: mysqladm
   13c Senha
14 Especifique mais informações de configuração para MySQL:
   14a Servidor de Nome Local: <nome de host da máquina local>
   14b Número da Porta CMS Padrão: 6400
15 Selecione: Install Tomcat (Instalar Tomcat)
16 Especifique as informações de configuração do Tomcat:
   16a Porta padrão de solicitações de HTTP de recebimento: 8080
   16b Porta padrão de solicitações de jsp de redirecionamento: 8443
   16c Porta padrão de hook de encerramento: 8005
17 Pressione Enter para confirmar o diretório padrão.
18 Pressione Enter para iniciar a instalação.
19 Observe o link para o servidor CMS, que será semelhante a:
   http://<nome de host>:8080/businessobjects/enterprise115/adminlaunch/launchpad.html

9.3 Publicando gabaritos do Crystal Reports

Observação: É altamente recomendável ler as Notas da Versão do Sentinel Reports antes de realizar a tarefa. Essas notas podem conter arquivos atualizados, scripts e etapas adicionais.

Muitos gabaritos de relatório são criados pela Novell para serem usados nas guias Análise e Advisor do Sentinel Control Center. Para fazer download do conjunto de relatórios mais recente, visite as páginas de conteúdo do Sentinel 6 na Web no seguinte URL:

http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html)

O conjunto básico de relatórios do Sentinel são distribuídos no Sentinel Core Solution Pack.

Você pode adicionar relatórios ao sistema de quatro maneiras:

- Faça download de um Solution Pack na guia Solution Packs e use o Gerenciador de Soluções para instalar um ou mais controles que incluam relatórios.
- Faça download de um Collector Pack na guia Coletores e use o Gerenciador de Soluções para instalar um ou mais controles que incluam relatórios.
- Adicione um ou mais gabaritos de relatório (arquivos .rpt) usando o Assistente de Publicação do Crystal.
- Adicione um ou mais gabaritos de relatório (arquivos .rpt) usando o Crystal Reports Central Management Console.

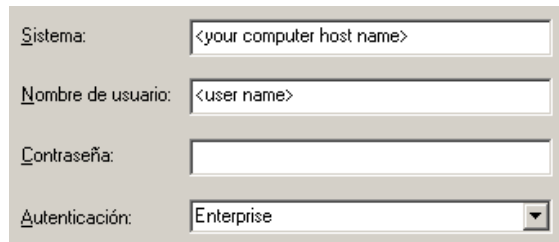
Importante: Para executar os 10 relatórios principais, habilite a agregação e ative o EventFileRedirectService no `DAS_Binary.xml`. Para obter informações sobre como habilitar a agregação, consulte a seção "Configuração de dados de relatório" de "Admin" no *Guia do Usuário do Sentinel*.

9.3.1 Publicando gabaritos de relatório com o Gerenciador de Soluções

Se você configurar corretamente o servidor web e o Crystal Reports Server usando as instruções de instalação descritas neste capítulo, os relatórios incluídos em um Solution Pack ou em um Collector Pack poderão ser publicados diretamente no Crystal Reports Server por meio do Gerenciador de Soluções. Para obter mais informações, consulte a "Solution Packs" no *Guia do Usuário do Sentinel*.

9.3.2 Publicando Gabaritos de Relatórios - Assistente de Publicação do Crystal Reports

Agora, os relatórios do Sentinel serão distribuídos por meio de Solution Packs, mas esse método poderá ser usado para publicar gabaritos de relatório provenientes de uma origem que não seja um Solution Pack.

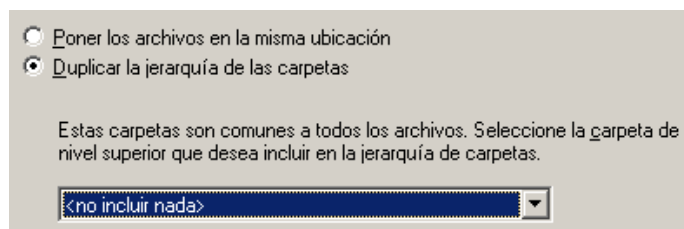
Observação: Uma plataforma Windows é obrigatória para a execução do Assistente de Publicação do Crystal Reports.

Para importar gabaritos do Crystal Reports:

Observação: Se você importar (publicar) os Gabaritos de Relatórios novamente, apague os gabaritos importados anteriormente.

---

1. Clique em Start (Iniciar) > All Programs (Todos os Programas) > BusinessObjects 115 > Crystal Reports Server > Assistente de Publicação.
2. Clique em Avançar.

Efetue login. Em Sistema, forneça o nome do computador host, e em Autenticação, especifique Enterprise. O Nome de Usuário pode ser Administrador. Por questões de segurança, não utilize o usuário Administrador, escolha outro. Forneça sua senha e clique em Avançar.

Observação: Relatórios publicados com o nome de usuário Administrador podem ser acessados por todos os usuários.

3 Clique em Adicionar Pasta. [Opcional] Clique em Incluir Subpastas.

4 Navegue para o local onde estão os gabaritos de relatório. Clique em OK. Clique em Next (Avançar).

5 Na janela Especificar Local, clique em Nova Pasta (canto superior direito) e crie uma pasta chamada SentinelReports (caso ela ainda não exista). Clique em Avançar.

6 Selecione:

- Duplicar hierarquia de pasta.
- Clique na seta para baixo e selecione <não incluir nenhum>.

Clique em Avançar.

7 Na janela Confirmar Localização, clique em Avançar.

8 Na janela Especificar Categorias, forneça o nome da categoria (como sentinel), realce o nome e clique no botão +.

Observação: Somente o primeiro relatório será exibido na categoria depois que você clicar em Avançar.

Clique em Avançar.

9. Na janela Especificar Programação, clique em Permitir que usuários atualizem o objeto (essa deve ser a opção padrão). Clique em Avançar.
10. Na janela Especificar Atualização do Repositório, clique em Habilitar Tudo para habilitar a atualização do repositório. Clique em Avançar.
11. Na janela Especificar Manutenção dos Dados Gravados, clique em Habilitar Tudo para manter os dados gravados quando publicar relatórios. Clique em Avançar.
12. Na janela Mudar Valores Padrão, clique em Publicar relatórios sem modificar propriedades (essa deve ser a opção padrão). Clique em Avançar.
13. Clique em Avançar para adicionar seus objetos.
14. Clique em Avançar. Clique em Concluir.

Quando forem publicados no Crystal Reports Server, os gabaritos do Sentinel para Crystal Reports deverão residir no diretório do SentinelReports; caso contrário, eles não serão exibidos no Sentinel Control Center.

9.3.3 Publicando gabaritos de relatório – Central Management Console

Agora, os relatórios do Sentinel serão distribuídos por meio de Solution Packs, mas esse método poderá ser usado para publicar gabaritos de relatório provenientes de uma origem que não seja um Solution Pack.

Para importar gabaritos do Crystal Reports:

1. Abra um browser da web e forneça o seguinte URL:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2. Clique em Central Management Console
3. Efetue login no Crystal Reports Server.
4. No painel Organize (Organizar), clique em Folders (Pastas).
5. No canto superior direito, clique em New Folder (Nova Pasta).
6. Crie a pasta SentinelReports (caso ela ainda não exista). Clique em OK.

Observação: É necessário que o nome da pasta seja SentinelReports.

7. Clique em SentinelReports.
8. Clique na guia Subpastas e crie subpastas se desejar. Se estiver adicionando os relatórios básicos do Sentinel manualmente, crie as seguintes subpastas:
   - Advisor_Vulnerability
   - Dashboards
   - Incident Management

- Internal Events
- Security Events
- Top 10

9. Clique em Home > Objects (Objetos) > New Object (Novo Objeto).
10. À esquerda da página, realce Report (Relatório).
11. Clique em Browse (Procurar) para procurar os gabaritos de relatório a serem adicionados. Escolha uma pasta e selecione um relatório.
12. Realce SentinelReports e clique em Show Subfolders (Mostrar Subpastas).
13. Selecione a pasta apropriada para o relatório e clique em Show Subfolders (Mostrar Subpastas).
14. Clique em Submit (Submeter).
15. Para adicionar os relatórios restantes, repita as etapas 9 até 17 até que todos os relatórios tenham sido adicionados.

9.4 Usando o servidor web Crystal XI R2

O Crystal Reports Server XI no Linux instala um servidor web com o qual você pode executar tarefas administrativas, além de publicar e ver relatórios.

O portal administrativo é acessado via browser no seguinte URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

O portal não-administrativo, ou de uso geral, é acessado via browser no seguinte URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115
```

9.4.1 Testando a conectividade com o servidor web

Para testar a conectividade com o servidor web:

1. Vá para outra máquina situada na mesma rede que o servidor web.
2. Forneça

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```

   Será exibida uma página da web do Crystal BusinessObjects.

9.4.2 Definindo uma conta de “Usuário Nomeado”

A chave de licença fornecida com o Crystal Reports Server é uma chave de Conta de Usuário Nomeado. A conta Guest foi mudada de Usuário Simultâneo para Usuário Nomeado.

Para definir a Conta Guest como Usuário Nomeado:

1. Abra um browser da web e forneça o seguinte URL:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2 Clique em Central Management Console.
3 O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.
4 No painel Organize (Organizar), clique em Users (Usuários) > Guest.
5 Mude o tipo de conexão de Concurrent User (Usuário Simultâneo) para Named User (Usuário Nomeado). Clique em Update (Atualizar).

   Efetue logoff e feche a janela.

9.4.3 Configurando permissões de relatórios

Esse procedimento discute como usar o Administration Launchpad para configurar as permissões de relatórios, de modo a permitir que você veja e modifique relatórios sob demanda.

Para configurar permissões de relatórios:

1 Abra um browser da web e forneça o seguinte URL:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2 Clique em Central Management Console.

   O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.
3 Forneça seu nome de usuário e sua senha e clique em Log On (Efetuar Login).
4 No painel Organize (Organizar), clique em Folders (Pastas).
5 Clique em SentinelReports e em Select All (Selecionar Tudo).
6 Clique na guia Rights (Direitos).
7 Em Everyone (Todos), no menu suspenso à direita, selecione View on Demand (Ver por Demanda).
8 Clique em Update (Atualizar) e em Logoff (Efetuar Logout) e, em seguida, feche a janela.

9.5 Aumentando o limite de registro de atualização do relatório do Crystal Reports Server

Se o Crystal tentar processar um número muito grande de eventos, você receberá um erro informando sobre o tempo máximo de processamento ou o limite máximo de registro. Para configurar o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server.

Para reconfigurar o Crystal Page Server:

1 Abra um browser da web e forneça o seguinte URL:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.
4. Forneça seu nome de usuário e sua senha e clique em Log On (Efetuar Login).
5. Clique em Servers (Servidores) e em <nome do servidor>.pageserver.
6. Em Database Records to Read When Previewing or Refreshing a report, (Registros do Banco de Dados para Ler ao Visualizar ou Atualizar um Relatório), selecione Unlimited records (Registros ilimitados e clique em Apply (Aplicar).
7. Você será solicitado a reiniciar o servidor de página. Clique em OK.
8. Talvez seja preciso fornecer um nome de login e uma senha para acessar o gerenciador de serviço do sistema operacional.

9.6 Configurando o Sentinel Control Center para integrar-se ao Crystal Reports Server

O Sentinel Control Center pode ser configurado para se integrar ao Crystal Reports Server. Isso permitirá que você veja o Crystal Reports a partir do Sentinel Control Center.

Para habilitar a integração do Sentinel Control Center com o Crystal Reports Server, siga as instruções abaixo.

Observação: Essa configuração só deverá ser executada depois que o Crystal Reports Server for instalado e que os relatórios do Crystal forem publicados nele. Para obter mais informações sobre plataformas suportadas para o Crystal Reports Server em ambientes Sentinel, consulte Capítulo 2, “Requisitos do sistema” na página 21.

Para configurar o Sentinel para se integrar ao Crystal Reports Server:

1. Efetue login no Sentinel Control Center como um usuário com privilégios na guia Admin.
2. Na guia Admin, selecione Configuração do Crystal Report.
3. No campo URL de Análise, forneça o seguinte:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Observação: <nome_de_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou pelo nome de host do Crystal Reports Server.

Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele precisa ser o nome do host.

Observação: <porta_padrão_do_servidor_web_8080> deve ser substituída pela porta de escuta do servidor web do Crystal.

---

4 Clique em Atualizar ao lado do campo URL de Análise.

5 Se o Advisor estiver instalado, forneça o seguinte no campo URL do Advisor:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Observação: `<nome_de_host_ou_IP_do_servidor_web>` deve ser substituído pelo endereço IP ou pelo nome de host do Crystal Reports Server.

Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele precisa ser o nome do host.

Observação: `<porta_padrão_do_servidor_web_8080>` deve ser substituída pela porta de escuta do servidor web do Crystal.

---

6 Clique em Atualizar ao lado do campo URL do Advisor.

Clique em Gravar.

7 Efetue logout e, em seguida, efetue login novamente no Sentinel Control Center.

As árvores do Crystal Reports nas guias Análise e Advisor (se o Advisor estiver instalado) agora aparecerão na janela Navegador.

9.7 Utilitários e solução de problemas

9.7.1 Iniciando o MySQL

Para verificar se o MySQL está em execução:

1 Efetue login como usuário crystal.

2 cd /opt/crystal_xir2/bobje

3 `./mysqlstartup.sh`

9.7.2 Iniciando o Tomcat

Para verificar se o Tomcat está em execução:

1 Efetue login como o usuário crystal.

2 cd /opt/crystal_xir2/bobje

3 `./tomcatstartup.sh`

9.7.3 Iniciando o Crystal Reports Servers

Para verificar se o Crystal Reports Servers está em execução:

1 Efetue login como o usuário crystal.

2 cd /opt/crystal_xir2/bobje

3 `./startservers`

9.7.4 Erro de nome de host Crystal

Para resolver o erro de nome de host:

1 Se receber este erro:

```
Warning: ORB::BOA_init: hostname lookup returned `localhost'
(127.0.0.1)
Use the -OAhost option to select some other hostname
```

Verifique se o IP e o nome de host estão no arquivo /etc/hosts. Por exemplo,

```
10.0.0.1   linuxCE02
```

9.7.5 Não é possível estabelecer conexão com o CMS

Se o sistema relatar que não é possível estabelecer conexão com o CMS, tente executar os comandos a seguir.

Para solucionar problemas da falha de conexão com o CMS:

1 Se o comando netstat –an | grep 6400 não retornar resultados, tente o seguinte:

- Forneça novamente informações sobre a conexão com o MySQL:
  1. Efetue login como o usuário crystal.
  2. cd /opt/crystal_xir2/bobje
  3. `./cmsdbsetup.sh`
  4. Pressione Enter quando `[<nome_de_host>.cms]` for exibido.
  5. Escolha selecionar e insira novamente todas as informações do banco de dados MySQL fornecidas durante a instalação. Para obter mais informações, consulte as instruções sobre instalação no Capítulo 3, “Instalando o Sentinel 6.1” na página 31.
  6. Quando terminar, saia de `cmsdbsetup.sh`.
  7. `./stopservers`
  8. `./startservers`
- Reinicialize o banco de dados MySQL:
  1. Efetue login como o usuário crystal.
  2. cd /opt/crystal_xir2/bobje
  3. `./cmsdbsetup.sh`
  4. Pressione Enter quando `[<nome_de_host>.cms]` for exibido.
  5. Selecione a opção de reinicialização e siga as instruções.
  6. Quando terminar, saia de `cmsdbsetup.sh`.

7. `./stopservers`
8. `./startservers`

1 Verifique se todos os servidores CCM estão habilitados:

1a Efetue login como o usuário crystal.

1b cd /opt/crystal_xir2/bobje

1c `./ccm.sh` -enable all

9.8 Configurações de alto desempenho para o Crystal

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para configurar o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server. Para fazer isso, use o Central Configuration Manager ou a página do Crystal na web.

Para reconfigurar o Crystal Page Server usando o Central Configuration Manager:

1 Clique em Start (Iniciar) > All Programs (Todos os Programas) > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.

2 Clique o botão direito do mouse em Crystal Reports Page Server e selecione Parar.

3 Clique o botão direito em Crystal Reports Page Server e selecione Propriedades.

4 Na guia Propriedades do campo Comando, no final da linha de comando, adicione:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the
default limit>
```

5 Reinicie o Crystal Page Server.

Para reconfigurar o Crystal Page Server usando o Central Management Console:

1 Clique em Start (Iniciar) > All Programs (Todos os Programas) > Businessobjects 11 > Crystal Reports Server > .Net Administration Launchpad. Como alternativa, você poder abrir um browser da web e fornecer o seguinte URL:

http://<Nome DNS ou endereço IP do servidor web>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx

2 Clique em Central Management Console.

3 O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Se não estiver, selecione Enterprise.

4 Forneça seu nome de usuário e sua senha e clique em Log On (Efetuar Login). Clique em Servers (Servidores).

5 Clique em <nome do servidor>.pageserver.

6 Em Database Records to Read When previewing or Refreshing a report (Registros do Banco de Dados para Ler quando Visualizar ou Atualizar um Relatório), selecione Unlimited records (Registros ilimitados). Clique em Apply (Aplicar).

7 Você será solicitado a reiniciar o servidor de página. Clique em OK.

Talvez seja preciso fornecer um nome de login e uma senha para acessar o gerenciador de serviço do sistema operacional.

9.8.1 Relatórios usando serviço de agregação

Para melhorar o desempenho, os 10 principais relatórios incluídos no Solution Pack do Sentinel Core consultam tabelas de resumo em vez de tabelas de eventos. As tabelas de resumo contêm contagens feitas ao longo do tempo para combinações de campos nos dados de eventos. Isso fornece um conjunto de dados muito menor para determinados tipos de consulta e resulta em consultas muito mais rápidas e tempos de execução de relatórios reduzidos.

O serviço de agregação é responsável pelo preenchimento das tabelas de resumo com resumos de todos os eventos da tabela de eventos. O serviço de agregação só gerará dados resumidos para resumos que ativos. Os resumos a seguir são exigidos pelos 10 principais relatórios e são habilitados por padrão:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Os resumos podem ser ativados ou desativados na janela Configuração de Dados de Relatório na guia Admin do Sentinel Control Center.

O serviço de agregação também depende do componente `EventFileRedirectService` do DAS Binary para alimentá-lo com os dados de eventos que serão resumidos. Portanto, esse componente deve ser habilitado para que o serviço de agregação seja executado adequadamente. Para habilitar ou desabilitar esse componente, modifique o atributo "status" do componente `EventFileRedirectService` do `das_binary.xml` para "on" (ativado) ou "off" (desativado). Por padrão, o status do componente está "on" (ativado).

Observação: Para obter informações sobre EventFileRedirectService e os três resumos de agregação, consulte "Configuração de dados de relatório" em Admin, no *Guia do Usuário do Sentinel*.

Observação: Os relatórios que consultam uma grande faixa de datas podem demorar para serem executados. Você pode programá-los em vez de executá-los interativamente. Para obter informações sobre como programar o Crystal Reports, consulte a documentação do Crystal Reports Server XI R2 (http://support.businessobjects.com/documentation/product_guides/default.asp).

9.8.2 Desenvolvimento do relatório

Você pode usar o Crystal Reports Developer para criar ou modificar relatórios. Para desenvolver relatórios personalizados, é recomendável o seguinte:

- Se os relatórios puderem utilizar tabelas agregadas predefinidas, selecione a tabela agregada resultante do processamento da menor quantidade de dados.
- Tente distribuir a maior parte do processamento de dados para o mecanismo de banco de dados.

- Para reduzir o overhead de processamento no Crystal Server, minimize a quantidade de dados a ser recuperada para o Crystal Server.
- Sempre grave relatórios nas telas do banco de dados fornecidas pela Novell, e não nas tabelas básicas.

Desinstalando o Sentinel

10

Para remover uma instalação do Sentinel, são fornecidos desinstaladores para Linux, Solaris e Windows. Vários arquivos, incluindo arquivos de registro, são preservados e podem ser removidos manualmente, se desejado. Antes de realizar uma nova instalação, é altamente recomendável que você execute todas as etapas a seguir para verificar se não restaram arquivos ou configurações do sistema de uma instalação anterior.

Aviso: Essas instruções envolvem a modificação de configurações e arquivos do sistema operacional. Se você não estiver familiarizado com a modificação dessas configurações e/ou arquivos do sistema, contate o Administrador do Sistema.

10.1 Desinstalando o Sentinel

10.1.1 Desinstalação no Solaris e no Linux

Para usar o desinstalador do Sentinel no Solaris e no Linux:

1. Efetue login como usuário root.
2. Pare o Sentinel Server.
3. Vá para:

   `$ESEC_HOME/_uninst`
4. Forneça:

   Para o modo de interface gráfica:

   `./uninstall.bin`

   Ou

   Para o modo baseado em texto ("serial console"):

   `./uninstall.bin -console`
5. Selecione um idioma e clique em OK.
6. O Assistente do Sentinel Install Shield é exibido. Clique em Avançar.
7. Selecione os componentes a serem desinstalados e clique em Avançar.
8. Pare todos os aplicativos do Sentinel que estiverem em execução e clique em Avançar.

9 Se tiver optado por desinstalar o componente de banco de dados, você será solicitado a selecionar uma das seguintes opções:
   - **Apagar toda a instância do banco de dados:** Remove a instância do banco de dados e libera o espaço em disco usado pelo banco de dados.
   - **Apagar apenas objetos do banco de dados:** Remove o conteúdo do banco de dados, com exceção do usuário esecdba. Em seguida, você poderá preencher a instância do banco de dados novamente usando o instalador do Sentinel. Essa opção não libera espaço em disco.

10 Se tiver selecionado Apagar apenas objetos do banco de dados, você será solicitado a fornecer a senha de esecdba. Clique em Avançar.

11 Será exibido um resumo dos recursos selecionados para desinstalação. Clique em Desinstalar.

12 Clique em Concluir.

10.1.2 Desinstalação no Windows

Para usar o desinstalador do Sentinel no Windows:

1 Efetue login como Administrador.

2 Pare o Sentinel Server.

3 Selecione Start (Iniciar) > All Programs (Todos os Programas) (Win XP) ou Programs (Programas) (WIN 2000)> Sentinel > Desinstalar Sentinel. Você também pode digitar %Esec_home%_uninst em Start (Iniciar) > Run (Executar) e clicar duas vezes em `uninstall.exe`.

4 Selecione um idioma e clique em OK.

5 O Sentinel 6.1 - Assistente do InstallShield é exibido. Clique em Avançar.

6 Selecione os componentes a serem desinstalados e clique em Avançar.

7 Pare todos os aplicativos do Sentinel que estiverem em execução e clique em Avançar.

8 Se tiver optado por desinstalar o componente de banco de dados, você será solicitado a selecionar uma das seguintes opções:
   - **Apagar todo o banco de dados:** Remove o banco de dados e libera o espaço em disco usado por ele.
   - **Apagar apenas objetos do banco de dados:** Remove o conteúdo do banco de dados, com exceção do usuário esecdba. Em seguida, você poderá preencher o banco de dados novamente usando o instalador do Sentinel. Essa opção não libera espaço em disco.

9 Se tiver optado por desinstalar o componente de banco de dados, você será solicitado a selecionar uma das seguintes opções:
   - **Autenticação do Windows:** Para usar a Autenticação do Windows, você deverá ter efetuado login no Windows como Administrador do Sistema de uma instância do MS SQL Server.
   - **Autenticação do SQL:** Forneça o nome de usuário e a senha do usuário sa (ou equivalente).

   Clique em Avançar.

10 Será exibido um resumo dos recursos selecionados para desinstalação. Clique em Desinstalar.

11 Reinicialize o sistema e clique em Concluir.

10.2 Pós-desinstalação

10.2.1 Configurações do Sentinel

Depois que você desinstalar o Sentinel, algumas configurações do sistema permanecerão e deverão ser removidas manualmente. Remova essas configurações antes de executar uma instalação “limpa” do Sentinel, particularmente se ocorrerem erros na desinstalação do programa.

Observação: No Solaris e no Linux, a desinstalação do Sentinel Server não removerá do sistema operacional o Usuário Administrador do Sentinel. Se desejar remover esse usuário, você deverá fazê-lo manualmente.

Remover configurações do sistema Sentinel no Linux

Para limpar manualmente o Sentinel no Linux:

1. Efetue login como usuário root.
2. Verifique se todos os processos do Sentinel foram parados.
3. Remova o conteúdo de /opt/novell/sentinel6 (ou do local onde o software Sentinel foi instalado).
4. Remova os arquivos de inicialização do Serviço do Sentinel:

   No SLES:

   ```
   chkconfig --del sentinel
   ```

   No RedHat:

   ```
   rm /etc/rc.d/rc0.d/K02sentinel
   rm /etc/rc.d/rc3.d/S98sentinel
   rm /etc/rc.d/rc5.d/S98sentinel
   ```

5. Remova os seguintes arquivos do diretório `/etc/rc.d/rc0.d`, caso eles existam:
   - K01wizard
   - K01esdee
   - K01esyslogserver
6. Remova os seguintes arquivos do diretório `/etc/rc.d/rc3.d`, caso eles existam:
   - S99wizard
   - S99esyslogserver
   - S99esdee
7. Remova os seguintes arquivos do diretório `/etc/rc.d/rc5.d`, caso eles existam:
   - S99wizard
   - S99esyslogserver
   - S99esdee
8. Remova os seguintes arquivos do diretório `/etc/init.d`, caso eles existam:
   - sentinel

- wizard
- esdee
- esyslogserver

9 Verifique se alguém está conectado ao sistema operacional como Administrador do Sentinel (o padrão é esecadm). Em seguida, remova o usuário (e o diretório pessoal) e o grupo esec.
   - Execute: `userdel -r esecadm`
   - Execute: `groupdel esec`

10 Remova o diretório /root/InstallShield.

11 Remova o arquivo /root/vpd.properties.

12 Remova a seção InstallShield de `/etc/profile e /etc/.login`.

13 Remova o banco de dados do Sentinel no Oracle. Para obter mais informações, consulte "Remover banco de dados do Sentinel do Oracle no Linux e no Solaris" na página 147.

14 Reinicie o sistema operacional.

Remover configurações do sistema Sentinel no Solaris

Para limpar manualmente o Sentinel no Solaris:

1 Efetue login como usuário root.

2 Verifique se há algum processo do Sentinel em execução.

3 Remova o conteúdo de `/opt/novell/sentinel6` (ou do local onde o software Sentinel foi instalado).

4 Remova os seguintes arquivos do diretório `/etc/rc0.d`, caso eles existam:
   - K01wizard
   - K02sentinel
   - K01esdee
   - K01esyslogserver

5 Remova os seguintes arquivos do diretório `/etc/rc3.d` , caso eles existam:
   - S98sentinel
   - S99wizard
   - S99esyslogserver
   - S99esdee

6 Remova os seguintes arquivos do diretório `/etc/init.d`, caso eles existam:
   - sentinel
   - wizard
   - esdee
   - esyslogserver

7 Remova os seguintes arquivos do diretório `/usr/local/bin`, caso eles existam:
   - `stop_wizard.sh`

- `restart_wizard.sh`
- `start_wizard.sh`

8. Verifique se alguém está conectado ao sistema operacional como Administrador do Sentinel. Em seguida, remova o usuário (e o diretório pessoal) e o grupo esec.
   - Execute: `userdel -r esecadm`
   - Execute: `groupdel esec`
9. Remova a seção InstallShield de `/etc/profile e /etc/.login`
10. Remova o diretório /InstallShield, caso ele exista.
11. Limpe as referências ao InstallShield em `/var/sadm/pkg.` Se os seguintes arquivos existirem, remova-os do diretório `/var/sadm/pkg`:
   - Todos os arquivos que começam com IS (IS* na linha de comando)
   - Todos os arquivos que começam com ES (ES* na linha de comando)
   - Todos os arquivos que começam com MISCwp (MISCwp* na linha de comando)
12. Remova o banco de dados do Sentinel no Oracle. Para obter mais informações, consulte "Remover banco de dados do Sentinel do Oracle no Linux e no Solaris" na página 147.
13. Reinicie o sistema operacional.

Remover banco de dados do Sentinel do Oracle no Linux e no Solaris

Para limpar manualmente o banco de dados do Sentinel do Oracle no Linux e no Solaris:

Observação: Verifique se nenhum outro aplicativo está usando esse banco de dados antes de removê-lo.

---

1. Efetue login como oracle.
2. Pare a escuta do Oracle:
   - Execute: `lsnrctl stop`
3. Pare o banco de dados do Sentinel:
   - Defina a variável de ambiente ORACLE_SID como o nome da instância do banco de dados do Sentinel (o padrão é ESEC).
   - Execute: `sqlplus "/ as sysdba"`
   - No prompt do sqlplus, execute: `shutdown immediate`
4. Remova a entrada referente ao banco de dados do Sentinel do arquivo oratab localizado em:

   No Linux:

   `/etc/oratab`

   No Solaris:

   `/var/opt/oracle/oratab`
5. Remova `init<nome_de_sua_ instância>.ora` (o padrão é `initESEC.ora`) do diretório $ORACLE_HOME/dbs.

6 Remova as entradas referentes ao banco de dados do Sentinel dos seguintes arquivos do diretório $ORACLE_HOME/network/admin:
   - `tnsnames.ora`
   - `listener.ora`
7 Apague os arquivos de dados contidos no banco de dados do local onde foram instalados.
8 Apague os arquivos mortos do banco de dados do local onde foram criados.

Remover configurações do sistema Sentinel no Windows com MS SQL Server

Para limpar manualmente o Sentinel do Windows:

1 Apague a pasta %CommonProgramFiles%\InstallShield\Universal e todo o seu conteúdo.
2 Apague a pasta %ESEC_HOME% (por padrão: C:\Arquivos de Programas\Novell\Sentinel6).
3 Clique o botão direito do mouse em My Computer (Meu Computador) > Porperties (Propriedades) > guia Advanced (Avançado).
4 Clique no botão Environment Variables (Variáveis de Ambiente).
5 Apague as seguintes variáveis, caso elas existam:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
6 Remova todas as entradas da variável de ambiente PATH que apontem para a instalação do Sentinel.

Aviso: Não remova caminhos que não sejam referentes à instalação antiga do Sentinel. Se remover outros caminhos, o sistema poderá apresentar problemas de funcionamento.

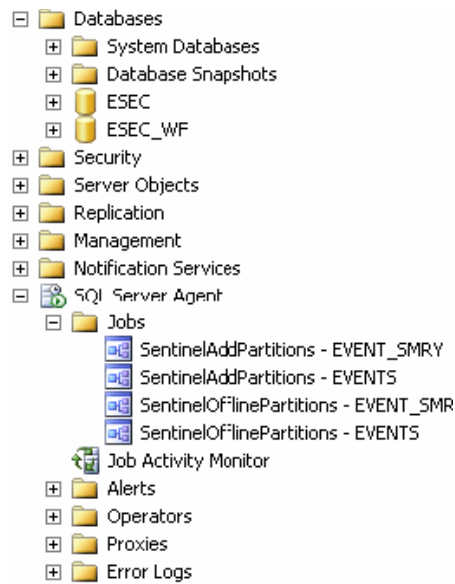
---

7 Apague da área de trabalho todos os atalhos do Sentinel.
8 Apague a pasta de atalhos Start (Iniciar) > Programs (Programas) > Sentinel do menu Start (Iniciar).
9 Reinicie o sistema operacional.

Para limpar manualmente o banco de dados do Sentinel do Microsoft SQL Server no Windows:

Observação: Verifique se nenhum outro aplicativo está usando esse banco de dados antes de removê-lo.

---

1 Abra o Microsoft SQL Server Management Studio e conecte a instância do SQL Server onde você instalou o banco de dados do Sentinel.

2 Expanda a árvore SQL Server Agent > Jobs e remova as tarefas do Sentinel.

3 Expanda a árvore Databases e localize seu banco de dados do Sentinel. Deverá haver um banco de dados do Sentinel (por padrão, chamado ESEC) e um banco de dados do iTRAC (por padrão, chamado ESEC_WF). Clique o botão direito do mouse em cada um deles e selecione Apagar (Excluir).

4 Ao ser solicitado, selecione Yes (Sim) para apagar o banco de dados.

5 Expanda a árvore Security > Login e remova os usuários do banco de dados do Sentinel, caso eles existam.

- esecdba
- esecapp
- esecadm
- esecrpt

6 Apague os arquivos mortos do banco de dados do local onde foram criados.

Questionário de pré-instalação

Responder a essas perguntas ajudará você a planejar sua própria instalação ou a preparar consultores para instalar seu sistema Sentinel.

Perguntas pré-instalação

1 Qual é seu objetivo ou propósito ao usar o Novell Sentinel?

1a Conformidade

1b Gerenciamento de eventos de segurança

1c Outros____

2 Qual hardware foi alocado para a instalação do Sentinel? Ele está de acordo com as especificações de hardware fornecidas no Guia de Instalação do Sentinel?

3 Você já validou o hardware do Sentinel e os requisitos do sistema operacional descritos no Guia de Instalação do Sentinel em sua configuração?

- Níveis de patch do sistema operacional
- Patches de serviços
- Hot Fixes, e assim por diante.

4 Sua máquina DAS atende aos requisitos de hardware e de sistema operacional necessários?

5 Qual é a arquitetura de rede para os dispositivos de origem com relação ao segmento de segurança no qual o hardware do Sentinel e do Coletor ficará localizado?

Observação: Isso ajudará você a compreender a hierarquia de coleta de dados do Coletor e a identificar que firewalls precisam ser atravessados para que seja possível habilitar a comunicação do Coletor com o Sentinel, do Sentinel com o banco de dados ou do Crystal Server com o banco de dados.

Forneça as informações abaixo (texto e/ou desenho) ou inclua um link para as informações.

6 Que relatórios você deseja retirar do sistema? Isso ajudará você a garantir que os Coletores coletem os dados corretos para serem passados para o banco de dados do Sentinel.

6a ______________________________

6b ______________________________

6c ______________________________

6d ______________________________

6e ______________________________

6f ______________________________

7 Em que dispositivos de origem você deseja coletar dados (IDS, HIDS, Roteadores, Firewalls, etc.), taxas de eventos (EPS - eventos por segundo), versões, métodos de conexão, plataformas e patches?

Dispositivo (mfr/modelo)	Taxa de eventos (EPS)	Versão	Método de conexão	Plataforma	Patches

Você pode oferecer exemplos dos dados a serem coletados e analisados pelos coletores do Sentinel? O Sentinel pode ser configurado para fornecer a saída desejada com base nas informações fornecidas aqui.

8 Quais padrões/modelos de segurança existem no seu site?

- Qual a sua postura em relação a contas locais versus autenticação de domínio?
  - Para Windows com autenticação de domínio, configurações apropriadas de conta de domínio devem ser criadas para garantir que o Sentinel possa ser instalado.
  - Isso não se aplica a instalações no Solaris. Contudo, o Sentinel não suporta NIS.

9 Qual a retenção de dados necessária por dia?

10 Com base nas informações de retenção de dados e EPS, qual tamanho de disco será usado? Use 500 a 800 bytes/evento para estimativas de tamanho.

11 Que padrões de evento deseja identificar em seus dados?

12 Os dados atuais disponíveis em suas origens de evento suportam os padrões de evento a serem detectados ou será necessário realizar o enriquecimento de eventos com o serviço de mapeamento?

13 Se for necessário usar o serviço de mapeamento, qual será a origem dos dados de enriquecimento e que chave será usada para a realização do mapeamento? Como os mapas serão mantidos atualizados?

14 Quando uma violação de segurança ou de conformidade for detectada, quais processos serão usados para correção?

Instalação do Oracle

B

B.1 Instalação do Oracle

Importante: ISENÇÃO DE RESPONSABILIDADE: A intenção das instruções fornecidas neste documento não é substituir a documentação do Oracle. Trata-se apenas de um exemplo de cenário de instalação. Esta documentação supõe que o diretório pessoal dos usuários do Oracle seja /home/oracle e que o Oracle será instalado em /opt/oracle. A configuração exata pode variar. Consulte a documentação do sistema operacional e do Oracle para obter mais informações.

Para obter mais informações sobre instalações do Oracle e para saber o nível de patch certificado ou suportado para o Sentinel, consulte a seção Capítulo 2, "Requisitos do sistema" na página 21.

B.1.1 Instalação do Oracle 10g no SLES 10

Para instalar o Oracle no SUSE Linux Enterprise Server 10:

1. Siga as instruções de instalação fornecidas no manual de instalação do SLES 10. Instale o SLES 10 com o sistema de arquivos ext3 e os pacotes padrão juntamente com o Oracle Server Base, o compilador C/C++ e as ferramentas.
2. Efetue login como usuário root.
3. Instale o SLES 10 Service pack. Para verificar as informações do service pack, digite:

   ```
   SPident
   ```

   ou

   ```
   cat /etc/SuSE-release
   ```

   Na data desta documentação, o SLES 10 service pack não havia sido lançado. Use SPident ou a versão cat/etc/SUSE para verificar.

   Você obterá:

   ```
   CONCLUSION: System is up-to-date!
     Found     SLES-10-x86_64-current
   ```

4. A conta do usuário oracle está desabilitada. Habilite-o mudando o shell do usuário oracle de /bin/false para /bin/bash, usando a administração de usuário do YaST ou editando o arquivo /etc/passwd.
5. Defina uma nova senha para o usuário oracle usando o YaST ou digitando:

   ```
   /usr/bin/passwd oracle
   ```

6. Se necessário, mude o ambiente padrão do Oracle definido por orarun:
   - Mude o diretório pessoal do Oracle editando a variável ORACLE_HOME no arquivo `/etc/profile.d/oracle.sh`.
   - O ORACLE_SID padrão definido pela instalação do orarun é 'orcl'. Mude-o para ESEC no arquivo `/etc/profile.d/oracle.sh`.
7. Para definir os parâmetros de kernel, execute

```
/usr/sbin/rcoracle start
```

8. Mude para o usuário oracle:

   ```
   su - oracle
   ```

9. Mude para diretório do banco de dados e execute `./runinstaller` (Oracle Universal Installer). Ocorrerá o seguinte erro:

10. Para corrigir o erro, execute um destes procedimentos:

    - Modifique o arquivo `database/install/oraparam.ni` para adicionar suporte ao SUSE Linux 10. Depois que você modificar o arquivo oraparam.ini, a linha "[Certified Versions]" ficará assim:

      ```
      [Certified Versions]
      Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-
      1,asianux-2
      ```

    - Instale com a opção -ignoreSysPrereqs

      ```
      that is ./runInstaller –ignoreSysPrereqs
      ```

11. Aceite o diretório de inventário padrão ou procure e selecione outro diretório. Clique em Next (Avançar).

12. Nos tipos de instalação, selecione Enterprise Edition. Clique em Next (Avançar).

13. Para verificar os requisitos de configuração de rede, selecione User Verified (Verificado pelo Usuário). Clique em Next (Avançar).

14. Nas opções de configuração, selecione Install Database Software (Instalar Software de Banco de Dados) apenas. Clique em Next (Avançar).

15. O resumo da instalação é exibido. Revise-o e clique em Install (Instalar).

16. Execute os scripts especificados como root e clique em OK ao concluir.

17. Após a instalação, clique em Exit (Sair).

B.1.2 Instalação do Oracle 10g no Red Hat Linux 4

Para instalar o Oracle no Red Hat Linux:

1. Efetue login como usuário root.

2. Execute o comando a seguir para verificar se os pacotes necessários (listados abaixo) estão instalados no servidor.

   ```
   rpm –q make
   ```

   Lista de pacotes:

   ```
   compat –db
   compat-gcc-32
   compat-gcc-32-c++
   compat-oracle-rhel4
   compat-libcwait
   compat-libgcc-296
   compat-libstdc++-296
   compat-libstdc++-33
   gcc
   gcc-c++
   gnome-libs
   gnome-libs-devel
   ```

```
libaio-devel
libaio
make
openmotif21
xorg-x11-deprecated-libs-devel
xorg-x11-deprecated-libs
```

3 Crie um grupo UNIX e uma conta de usuário UNIX para o proprietário do banco de dados Oracle.

Adicione um grupo dba (como root):

```
groupadd oinstall
groupadd dba
```

4 Adicione o usuário do Oracle (como root):

```
useradd –g oinstall –G dba –d /opt/oracle/product/<10.2.0.3>/db_1 –
m oracle
passwd oracle
```

5 Crie um diretório para ORACLE_HOME e ORACLE_BASE:

```
mkdir –p /opt/oracle/product/<10.2.0.3>
```

6 Mude a propriedade do diretório ORACLE_BASE e complete para o oracle/oinstall:

```
chown -R oracle:oinstall /opt/oracle
```

7 Mude para o usuário oracle:

```
su - oracle
```

8 Abra o arquivo `.bash_profile` (no diretório pessoal do usuário oracle) para editá-lo e adicione o seguinte ao final do arquivo:

Observação: Esse conjunto de variáveis de ambiente só deve ser usado para o usuário oracle. Mais especificamente, essas variáveis não devem ser definidas no ambiente de sistema nem no ambiente de Usuário do Administrador do Sentinel.

```
# User specific environment and startup programs
ORACLE_BASE=/opt/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/10.2.0/db_1; export ORACLE_HOME
ORACLE_TERM=xterm; export ORACLE_TERM
PATH=$ORACLE_HOME/bin:$PATH; export PATH
ORACLE_SID=oracle; export ORACLE_SID
LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/JRE:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/
jlib
CLASSPATH=$CLASSPATH:$ORACLE_HOME/network/jlib; export CLASSPATH
LD_ASSUME_KERNEl=2.4.19; export LD_ASSUME_KERNEL
TMP=/tmp; export TMP
TMPDIR=$TMP;export TMPDIR
PATH=$PATH:$HOME/bin
export PATH

unset USERNAME
```

9 Grave o `.bash_profile` e saia.

10 Repita o login como usuário oracle para carregar as mudanças de variáveis de ambiente feitas depois da última etapa:

```
exit
su - oracle
```

11 Verifique se `.bash_profile` foi executado conforme o esperado. Para isso, use este comando:

```
set | more
```

12 Efetue login como usuário Oracle. Se estiver usando a emulação X, defina a variável de ambiente DISPLAY:

```
DISPLAY=<machine-name>:0.0; export DISPLAY
```

13 Para instalar o Oracle 10.2.0.1 usando Disk1, execute o script:

```
./runInstaller
```

14 Ao avançar no instalador, deixe todos os prompts com seus valores padrão, exceto se houver especificação em contrário.

- Na janela de boas-vindas, clique em Next (Avançar).
- Na janela File Locations (Localizações de Arquivos), selecione OUIHome no menu suspenso de Destination Name (Nome de Destino). Clique em Next (Avançar).
- Dependendo da versão, na janela Select Product to Install (Selecionar Produto para Instalação), selecione Oracle 10g Banco de Dados 10.2.0.1 e clique em Next (Avançar).
- Na janela Installation Types (Tipos de Instalação), selecione Enterprise Edition. Clique em Next (Avançar).
- Na janela Database Configuration (Configuração do Banco de Dados), selecione General Purpose (Finalidade Geral). Clique em Next (Avançar).
- Na janela Summary (Resumo), revise o resumo de instalação e clique em Install (Instalar).
- Na janela End of Installation (Fim da Instalação), clique em Exit (Sair).

15 Para aplicar o patch do Oracle 10.2.0.3 usando o Disk1 da distribuição de patch do Oracle 10.2.0.3, execute o script:

```
./runInstaller
```

16 Siga os prompts nas janelas de instalação. Na janela Summary (Resumo), revise o resumo de instalação e clique em Install (Instalar). Na janela End of Installation (Fim da Instalação), clique em Exit (Sair).

B.1.3 Instalação do Oracle 10g no Solaris 10

Observação: Para obter mais informações sobre os procedimentos a serem seguidos para configurar o parâmetro de kernel no Solaris 10, consulte Seção 3.4.1, “Definindo valores do Kernel” na página 39.

Para instalar o Oracle 10g no Solaris 10:

1 Efetue login como usuário root.

2 Inicie a instalação.

```
#  su - oracle
# < Installation directory or CD mount>/ .runInstaller
```

3 Na janela de boas-vindas:

- Selecione Basic Installation (Instalação Básica).

- Desmarque a opção Create Starter Database (Criar Banco de Dados de Início).
- Especifique a localização inicial do Oracle.
- Geralmente, o Grupo DBA do UNIX é dba. Clique em Next (Avançar).

4 Na janela Product-Specific Prerequisite (Pré-requisito Específico do Produto):

- Verifique se todas as verificações de sistema foram bem-sucedidas. Clique em Next (Avançar).

5 Na janela de resumo:

- Revise o resumo de instalação e clique em Install (Instalar).
- Na janela End of Installation (Fim da Instalação), clique em Exit (Sair).

B.2 Criação manual de instância do Oracle (opcional)

Para simplificar, a Novell recomenda que você use o instalador do Sentinel para criar a instância do Oracle durante a instalação dos componentes do banco de dados do Sentinel. No entanto, esse procedimento é fornecido pois a política da empresa pode exigir que o DBA crie a instância do Oracle. Os nomes dos tablespaces devem seguir exatamente as especificações fornecidas.

Na instância Oracle, será necessário configurar:

- Parâmetros
- Tablespaces

Para criar uma instância do Oracle:

1 Efetue login como usuário Oracle.

2 Use a interface gráfica do Database Assistant (Assistente de Banco de Dados) do Oracle para criar o seguinte:

Observação: Os valores podem variar dependendo da configuração e dos requisitos do sistema. Consulte o DBA.

Tabela B-1 *Parâmetros mínimos recomendados para configuração do Solaris/Linux*

Parâmetros mínimos recomendados para configuração do Solaris/Linux	
Parâmetros	**Tamanho (bytes ou outra especificação)**
db_cache_size	1 GB
java_pool_size	33.554.432
large_pool_size	8.388.608
shared_pool_size	100 MB
pga_aggregate_target	150.994.944
sort_area_size	109.051.904
open_cursors	500

Parâmetros mínimos recomendados para configuração do Solaris/Linux	
Parâmetros	**Tamanho (bytes ou outra especificação)**
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tabela B-2 *Tamanho mínimo recomendado para tablespace Solaris/Linux*

Tamanho mínimo recomendado para tablespace Solaris/Linux		
Tablespace	**Exemplo de tamanho**	**Notas**
REDO	3x100M	Valor mínimo. Deverá ser aumentado se a taxa de eventos for alta.
SYSTEM	500M	Valor mínimo (autoextend habilitado)
TEMP	1G	Valor mínimo (autoextend habilitado)
UNDO	1G	Valor mínimo (autoextend habilitado)
ESENTD	5G	Valor mínimo Para dados de eventos (autoextend habilitado)
ESENTD2	500M	Valor mínimo Dados de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
ESENTWFD	250M	Para dados do iTrac (autoextend habilitado)
ESENTWFX	250M	Para índice do iTrac (autoextend habilitado)
ESENTX	3G	Valor mínimo Para índice de eventos (autoextend habilitado)
ESENTX2	500M	Valor mínimo Índice de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
SENT_ADVISORD	15G	Valor mínimo se o Advisor for comprado. Para dados do Advisor (autoextend habilitado).
SENT_ADVISORX	15G	Valor mínimo se o Advisor for comprado. Para índice do Advisor (autoextend habilitado)
SENT_AUDITD	250M	Valor mínimo Para dados de auditoria do Sentinel (autoextend habilitado)

Tablespace	Exemplo de tamanho	Notas
SENT_AUDITX	250M	Valor mínimo Para índice de auditoria do Sentinel (autoextend habilitado)
SENT_LOBS	100M	Valor mínimo na instalação básica Para objetos Bancos de Dados grandes (autoextend habilitado)
	2G	Valor mínimo na instalação se a integração com o sistema de gerenciamento de identidade estiver habilitado. Para objetos Bancos de Dados grandes (autoextend habilitado)
SENT_SMRYD	3G	Valor mínimo Para agregação, dados de resumo (autoextend habilitado)
SENT_SMRYX	2G	Valor mínimo Para agregação, índice de resumo (autoextend habilitado)
SYSAUX	100M	Valor mínimo Para auditoria do Oracle 10g (não é específico do Sentinel) Necessário somente para Oracle 10g

Tamanho mínimo recomendado para tablespace Solaris/Linux

3. Execute o script `createEsecdba.sh` encontrado no diretório sentinel\dbsetup\bin no CD de Instalação do Sentinel. Esse script criará o usuário esecdba, que é necessário para a adição de objetos Bancos de Dados com o instalador do Sentinel.
4. Faça backup do banco de dados.

Para obter mais informações sobre a instalação de bancos de dados em um banco de dados existente, consulte a seção Capítulo 3, “Instalando o Sentinel 6.1” na página 31.

Sentinel com RAC (Real Application Clusters) do Oracle

C

O Sentinel 6 está certificado para ser executado em um banco de dados Oracle com RAC (Real Application Clusters). A versão suportado do banco de dados Oracle é Oracle 10g Versão 2 (64 bits) com RAC (Real Application Clusters).

Além dos procedimentos de instalação padrão do Sentinel, você deve seguir algumas etapas adicionais para instalar e configurar o Sentinel para usar o RAC do Oracle:

- Configure o banco de dados RAC do Oracle
- Instale o esquema do Banco de Dados do Sentinel no RAC do Oracle
- Configure os arquivos de propriedades de conexão para componentes do DAS
- Configure a conexão do Gerenciador de Dados do Sentinel
- Configure a conexão do Crystal Enterprise Server

Essas etapas são descritas neste documento.

Observação: Antes de instalar o software Sentinel 6.0, verifique se o cluster do Oracle está em execução usando ferramentas RAC do Oracle.

C.1 Configurando o banco de dados RAC do Oracle

Para configurar o banco de dados RAC do Oracle:

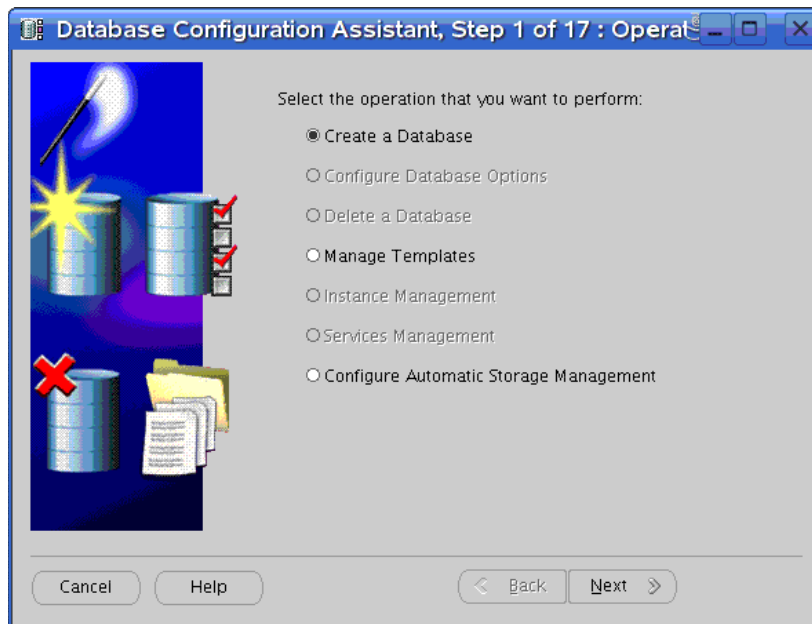
- Crie o banco de dados RAC usando o utilitário Oracle Database Configuration Assistant (Assistente de Configuração de Banco de Dados Oracle)
- Crie os tablespaces do Sentinel necessários para conter dados do Sentinel
- Crie o proprietário de esquema do Sentinel ESECDBA
- Instale o banco de dados do Sentinel
- Instale os componentes restantes do Sentinel
- Configure o arquivos de propriedades de conexão

C.1.1 Criando o banco de dados RAC

Esse procedimento criará um banco de dados RAC do Oracle vazio, pronto para a instalação dos componentes do Sentinel. Além disso, esse procedimento usa o Oracle Database Configuration Assistant (DBCA).

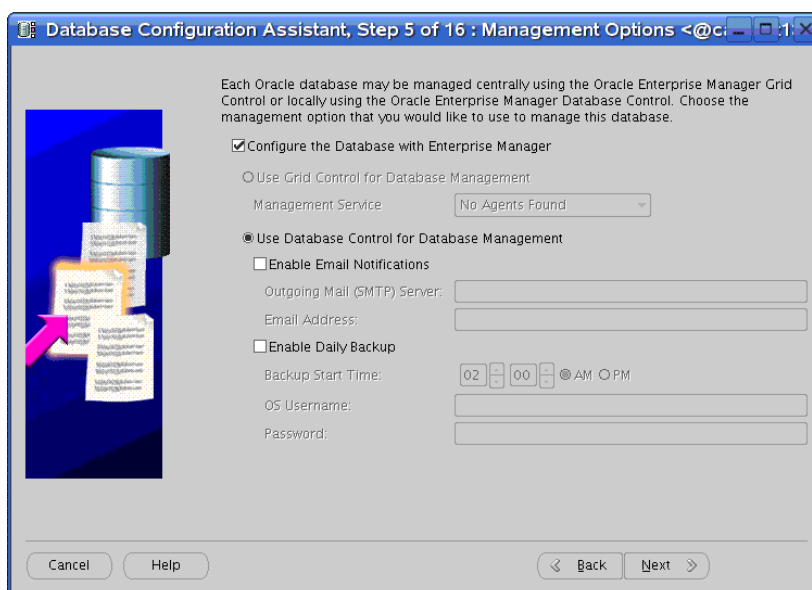
Para criar o banco de dados RAC:

1 Selecione o banco de dados RAC do Oracle no Database Configuration Assistant (Assistente de Configuração de Banco de Dados). Clique em Next (Avançar).

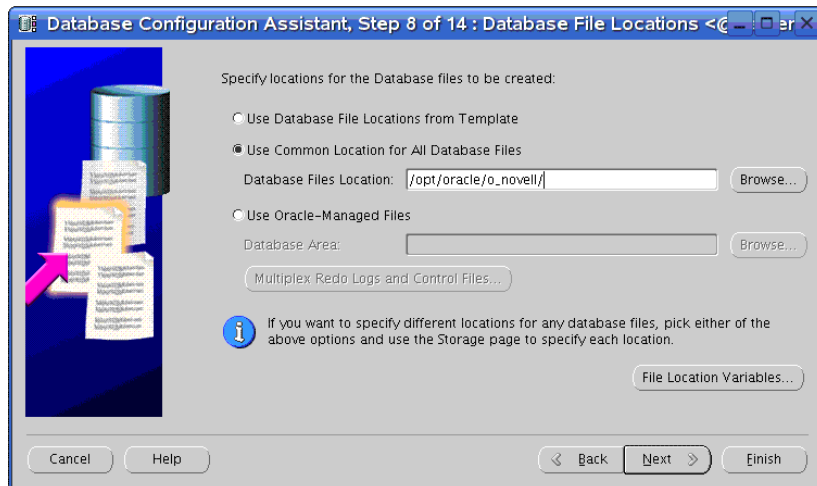
2 Nas opções exibidas na tela, selecione Create a database (Criar um banco de dados). Clique em Next (Avançar).

3 Para selecionar todos os nós para criar o banco de dados de cluster, clique em Select All (Selecionar Tudo). Clique em Next (Avançar).

4 Selecione uma opção na lista de gabaritos. Por padrão, o gabarito General Purpose (Finalidade Geral) é selecionado. Clique em Next (Avançar).

5 Forneça o nome do banco de dados e o prefixo do SID (identificador do sistema Oracle). Clique em Next (Avançar).

6 A opção de gerenciamento padrão selecionada para gerenciar esse banco de dados é Configure the Database with Enterprise Manager (Configurar o Banco de Dados com o Enterprise Manager). Clique em Next (Avançar).

7 Você pode usar as mesmas senhas para todas as contas de usuário ou pode escolher senhas diferentes. Escolha sua opção e forneça as senhas. Clique em Next (Avançar).

8 Nos três mecanismos de armazenamento oferecidos pelo sistema, Cluster File System (Sistema de Arquivos de Cluster)/Automatic Storage Management (Gerenciamento de Armazenamento Automático)/Raw Devices (Dispositivos Não Processados), selecione a opção desejada. Se escolher Raw Devices (Dispositivos Não Processados), especifique o caminho do arquivo de mapeamento de Raw Devices (Dispositivos Não Processados). Clique em Next (Avançar).

9 Especifique em que diretório do sistema de armazenamento os arquivos de banco de dados devem ser colocados. Clique em Next (Avançar).

10 Mantenha a seleção padrão nas opções de recuperação e nas janelas Sample Schemas (Exemplos de Esquema) e clique em Next (Avançar).

11 Você pode criar um Database Service (Serviço de Banco de Dados) nesse momento ou mais tarde usando o DBCA.

12 Na janela Database storage (Armazenamento de banco de dados), mantenha a seleção padrão. Clique em Next (Avançar).

13 Nas opções de criação de bancos de dados, selecione Create Database (Criar Banco de Dados). Clique em Finish (Concluir).

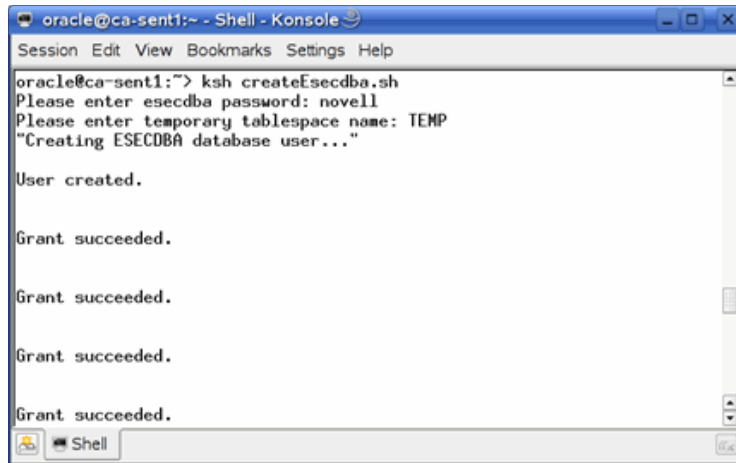
C.1.2 Criando tablespaces do Sentinel

Aviso: A instalação do Sentinel não será bem-sucedida se algum dos tablespaces abaixo não for criado.

Observação: Você pode usar o Oracle Enterprise Manager ou a consulte SQL para verificar a existência desses tablespaces.

Tabela C-1 Tamanho mínimo recomendado para tablespace

Tamanho mínimo recomendado para tablespace		
Tablespace	**Exemplo de tamanho**	**Notas**
Tamanho mínimo recomendado para tablespace		
REDO	3 x 100M	Este é o valor mínimo. Você deverá criar redo logs maiores se a taxa de eventos for alta.
SYSTEM	500M	Valor mínimo (autoextend habilitado)
TEMP	1G	Valor mínimo (autoextend habilitado)
UNDO	1G	Valor mínimo (autoextend habilitado)
ESENTD	5G	Valor mínimo
		Para dados de eventos (autoextend habilitado)
ESENTD2	500M	Valor mínimo
		Dados de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
ESENTWFD	250M	Para dados do iTRAC (autoextend habilitado)
ESENTWFX	250M	Para índice do iTRAC (autoextend habilitado)
ESENTX	3G	Valor mínimo
		Para índice de eventos (autoextend habilitado)
ESENTX2	500M	Valor mínimo
		Índice de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
SENT_ADVISORD	15G	Valor mínimo se o Advisor for comprado
		Para dados do Advisor (autoextend habilitado)
SENT_ADVISORX	15G	Valor mínimo se o Advisor for comprado
		Para índice do Advisor (autoextend habilitado)
SENT_AUDITD	250M	Valor mínimo
		Para dados de auditoria do Sentinel (autoextend habilitado)
SENT_AUDITX	250M	Valor mínimo
		Para índice de auditoria do Sentinel (autoextend habilitado)

Tamanho mínimo recomendado para tablespace		
Tablespace	**Exemplo de tamanho**	**Notas**
SENT_LOBS	100M	Valor mínimo na instalação básica
		Para objetos Bancos de Dados grandes (autoextend habilitado)
	2G	Valor mínimo na instalação se a integração com o sistema de gerenciamento de identidade estiver habilitado.
		Para objetos Bancos de Dados grandes (autoextend habilitado)
SENT_LOBS	100M	Valor mínimo
		Para objetos Bancos de Dados grandes (autoextend habilitado)
SENT_SMRYD	3G	Valor mínimo
		Para agregação, dados de resumo (autoextend habilitado)
SENT_SMRYX	2G	Valor mínimo
		Para agregação, índice de resumo (autoextend habilitado)
SYSAUX	100M	Valor mínimo
		Para auditoria do Oracle 10g (não é específico do Sentinel)

C.1.3 Criando o ESECDBA

ESECDBA é o nome do proprietário do esquema do Sentinel. Esse usuário será o proprietário da maioria dos objetos criados pelo instalador do Sentinel.

Para criar o ESECDBA:

1. Localize o script `createEsecdba.sh` no disco de instalação do Sentinel, em disk1/sentinel/dbsetup/bin.
2. Execute esse script em qualquer máquina com o cliente Oracle instalado. Talvez seja necessário editar o script para definir adequadamente as variáveis de ambiente do Oracle e a string “CONNECT AS” (por padrão, o script é conectado como “sysdba”).

   Aviso: Só execute esse script uma vez.

C.2 Instalando o Banco de Dados do Sentinel

Depois de configurar o banco de dados, instale o banco de dados do Sentinel. Este procedimento realizará a instalação em um único nó do cluster, como se fosse uma instância não-RAC do Oracle.

Você pode executar o instalador do Sentinel em qualquer máquina com o cliente Oracle instalado, desde que as variáveis de ambiente do Oracle contidas no sistema estejam definidas para o usuário "oracle" (ORACLE_HOME, ORACLE_BASE). Se essa máquina também for o Sentinel Server, você poderá instalar esses componentes simultaneamente (consulte acima as seções sobre prompts dos componentes básicos).

Para instalar o banco de dados do Sentinel:

1. Efetue login no servidor de instalação como usuário root.
2. Insira e monte o conjunto de arquivos ou o CD de instalação do Sentinel.
3. Procure o CD e clique duas vezes:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   Para modo textual ("sem cabeçalho"):

   ```
   ./setup.sh -console
   ```
4. Selecione o idioma e clique em OK.
5. Depois de ler a tela de boas-vindas, clique em Avançar.
6. Leia e aceite o Contrato de Licença de Usuário Final e clique em Avançar.
7. Aceite o diretório de instalação padrão ou clique em Procurar para especificar um local diferente. Clique em Avançar.
8. No tipo de instalação, selecione Personalizada (padrão). Clique em Avançar.
9. Na janela de seleção de recursos, desmarque todas as opções desnecessárias e selecione Banco de Dados. Clique em Avançar.
10. Selecione a plataforma de servidor do banco de dados de destino.
    - Selecione Oracle 10g na lista suspensa.
    - Selecione Adicionar objetos Banco de Dados a um banco de dados existente.

Clique em Avançar.

11. Forneça informações de autenticação para criar:
    - Usuário de Banco de Dados do Aplicativo Sentinel
    - Usuário do Administrador do Sentinel

    Clique em Avançar.
12. O resumo de parâmetros de Banco de Dados especificados é exibido. Clique em Avançar.
13. O resumo da instalação é exibido. Clique em Instalar.
14. Após a instalação, clique em Concluir.
15. Instale o restante do sistema Sentinel (inclusive o Collector Services, o DAS, o Servidor de Comunicação e outros componentes do Sentinel) usando as informações contidas no Capítulo 3, "Instalando o Sentinel 6.1" na página 31.

C.3 Configurando arquivos de propriedades de conexão

Você precisa criar manualmente um arquivo de propriedades de conexão de banco de dados usando as informações de conexão do banco de dados RAC. O arquivo de propriedades de conexão de banco de dados deve ser criado na mesma máquina em que o DAS (Serviço de Acesso a Dados) foi instalado. Parte das informações necessárias pode ser encontrada no arquivo $ORACLE_HOME/db/network/admin/tnsnames.ora, nos nós do cluster.

Para configurar RACconnect.properties:

1. Efetue login na máquina em que os componentes do DAS (Serviço de Acesso a Dados) do Sentinel estão instalados.
2. Mude o diretório para $ESEC_HOME/config.
3. Crie o arquivo RACconnect.properties. Veja a seguir um exemplo configurado para um serviço chamado OLTP com três nós:

```
driver=esecurity.base.db.driver.OracleProxyDriver
dburl=jdbc:esecurity:oracleproxy:@
realdriver=oracle.jdbc.driver.OracleDriver
realdburl=jdbc:oracle:thin:@
fatalvendorstates=28,600,1012,1014,1033,1034,1035,1089,1090,1092,1
094,2396,3106,3111,3113,3114
advancedconnectionstring=(DESCRIPTION=
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent1.novell.com) (PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent2.novell.com) (PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent3.novell.com) (PORT=1521))
(LOAD_BALANCE=yes)
(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=OLTP)
(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC)(RETRIES=180)
(DELAY=5))))
```

    Observação: O valor "advancedconnectionstring" deve ficar em uma única linha.

    ---
4. Edite o arquivo `configuration.xml` em $ESEC_HOME e adicione os seguintes argumentos aos componentes do processo listados abaixo:

```
-Desecurity.connect.config.file=../config/RACconnect.properties
```

Estes são alguns dos componentes do processo que precisam dessa mudança:

- DAS_Aggregation
- DAS_Binary
- DAS_iTRAC
- DAS_Query
- DAS_RT

Por exemplo:

```
<process component="DAS" depends="UNIX Communication
Server,Windows Communication Server" image=""$(ESEC_JAVA_HOME)/
java" -server -Dsrv_name=DAS_Query
-Xmx256m -Xms85m -XX:+UseParallelGC -Xss136k -Xrs
-Duser.language=en -Dfile.encoding=UTF8
-Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml,
/xml/WorkflowMetaData.xml
-Djava.util.logging.config.file=../config/das_query_log.prop
-Djava.security.auth.login.config=../config/auth.login
-Djava.security.krb5.conf=../config/krb5.conf
-Desecurity.execution.config.file=../config/execution.properties -
Dcom.esecurity.configurationfile=../config/configuration.xml
-Desecurity.connect.config.file=../config/RACconnect.properties
-jar ../lib/ccsbase.jar ..//config//das_query.xml"
min_instances="1" name="DAS_Query" post_startup_delay="20"
type="container" working_directory="$(ESEC_HOME)/data" />
```

5. Reinicie os serviços do Sentinel para que as mudanças feitas na conexão do banco de dados entrem em vigor.

C.4 Configurando a conexão do Gerenciador de Dados do Sentinel

Use o valor advancedconnectionstring do arquivo RACconnect.properties para efetuar login no Gerenciador de Dados do Sentinel.

Para efetuar login no Gerenciador de Dados do Sentinel:

1. Inicie o Gerenciador de Dados do Sentinel a partir de $ESEC_HOME/bin/sdm.
2. Forneça o nome de usuário e a senha do Administrador do Banco de Dados do Sentinel (o padrão é esecdba).
3. Copie o valor advancedconnectionstring do arquivo RACconnect.properties.
4. Cole o valor advancedconnectionstring no campo String de Conexão.
5. Grave as configurações de conexão.
6. Clique em Conectar.

Um banco de dados MSSQL será criado com os seguintes parâmetros:
Será criado um novo banco de dados com o nome: **ESEC**
Este banco de dados terá um tamanho inicial de **1000 MB**.
Esse banco de dados terá o tamanho máximo de **10000 MB**.

As localizações dos armazenamentos dos arquivos de dados serão as seguintes:
Arquivos de Dados: **C:\Arquivos de programas\Novell\Sentinel6\database**
Arquivos de Índice: **C:\Arquivos de programas\Novell\Sentinel6\database**
Arquivos de Dados de Resumo: **C:\Arquivos de programas\Novell\Sentinel6\database**
Arquivos de Índice de Resumo: **C:\Arquivos de programas\Novell\Sentinel6\database**
Arquivos de Registro: **C:\Arquivos de programas\Novell\Sentinel6\database**

O proprietário do esquema será: **esecdba**
O usuário do Aplicativo Sentinel será: **$v(Esec_APP_LOGIN)**
O Administrador do Sentinel será: **esecadm**
O Usuário do Sentinel Report será: **esecrpt**

C.5 Configurando a conexão do Crystal

Para que o Crystal Enterprise Server use o banco de dados RAC do Oracle, você deve editar o arquivo tnsnames.ora. Siga as etapas da instalação padrão do Crystal Enterprise Server antes de executar estas etapas.

Para editar o arquivo tnsnames.ora:

1. Efetue login no servidor em que o Crystal Enterprise Server está instalado e localize o arquivo tnsnames.ora.
2. Modifique o serviço ESECURITYDB para que mostre informações de todos os nós. O endereço IP deve ser o endereço IP virtual. Veja a seguir um exemplo de arquivo de sistema com três nós:

```
ESECURITYDB =
 (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.1)(PORT = 1521))
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.2)(PORT = 1521))
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.3)(PORT = 1521))
   (LOAD_BALANCE = yes)
   (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = REPORT.novell.com)
     (FAILOVER_MODE =
       (TYPE = SELECT)
       (METHOD = BASIC)
       (RETRIES = 180)
       (DELAY = 5)
     )
   )
)
```